

# 网络空间作战：机理与筹划

敖志刚 编著

電子工業出版社

Publishing House of Electronics Industry

北京 • BEIJING

## 内 容 简 介

本书系统地反映了网络空间作战的精髓、核心内容、基本原理、战略筹划、战术技术、方式方法、体制机制、力量建设、体系结构、任务要求、过程描述、解决方案、研究现状和最新发展方向。其主要内容涉及网络空间的作战基础、美军作战战略和指挥与控制体系、作战武器、网络靶场规划及其建设、态势感知、进攻性作战、防御性作战、进攻源追踪、作战指挥与控制等方面。

本书适用于业余爱好者自学,可作为高校学生选修课和专业培训的教材或教学参考书,也可作为学习网络安全、网络空间攻防、信息作战和网络中心战的本科生和研究生的必修课教材或教学参考书,还可供从事网络安全、网络空间作战研究、教学、规划、设计、开发、管理的科研人员、教师和工程技术人员阅读与参考。

未经许可,不得以任何方式复制或抄袭本书之部分或全部内容。  
版权所有,侵权必究。

### 图书在版编目(CIP)数据

网络空间作战:机理与筹划/敖志刚编著. —北京:电子工业出版社,2018.9  
ISBN 978-7-121-33803-8

I. ①网… II. ①敖… III. ①计算机网络—应用—作战—研究 IV. ①E83-39

中国版本图书馆CIP数据核字(2018)第042513号

责任编辑:李树林

印 刷:

装 订:

出版发行:电子工业出版社

北京市海淀区万寿路173信箱 邮编 100036

开 本:787×1092 1/16 印张:34.75 字数:890千字

版 次:2018年9月第1版

印 次:2018年9月第1次印刷

定 价:138.00元

凡所购买电子工业出版社图书有缺损问题,请向购买书店调换。若书店售缺,请与本社发行部联系,联系及邮购电话:(010)88254888,88258888。

质量投诉请发邮件至 [zltz@phei.com.cn](mailto:zltz@phei.com.cn), 盗版侵权举报请发邮件至 [dbqq@phei.com.cn](mailto:dbqq@phei.com.cn)。

本书咨询和投稿联系方式:(010)88254463, [lisl@phei.com.cn](mailto:lisl@phei.com.cn)。

# 前言



网络空间是一个由各要素通过组网所形成的广阔领域，既包括电磁空间和人参与的虚拟环境，也包括由互联网、无线网、电信网、物联网、计算机系统、武器装备系统、军事指挥与控制网、金融网、电力交通网等组成的空间。网络空间与陆、海、空、天并列为五大作战空间。

网络空间每天都与每个人息息相关，人们的学习、工作、生活、休闲、购物等越来越需要网络空间，甚至网络空间还关系着人们的生存。在网络空间，美国是第一强国，掌控全球计算机和互联网的核心技术和重要应用；中国则是第一大国，拥有最多的网民数量和最大的产业市场。截至 2017 年 6 月，我国互联网宽带接入端口数量达 7.39 亿个，中国手机网民规模达 7.24 亿人；全球超过一半人口使用互联网。网络空间已经开始向世界各个角落辐射，正在成为承载政治、经济、文化、外交、军事的全新空间。

网络空间的发展带来了机遇，也带来了风险和威胁。网络空间的安全问题已经成为信息时代国家安全的核心内容之一，直接影响社会稳定、国家安全、经济发展和文化传播，直接挑战社会管理、公众权益和世界和平。2014 年，中共中央网络安全和信息化领导小组明确提出了“没有网络安全就没有国家安全”的论断。保护网络空间是一项要求所有人都积极参与的复杂事业。我们的任务是：筑牢网络安全堤坝，共建网络安全防线，强化网络安全意识，守住网络安全底线，开展网络安全侦测，完善网络安全机制，惩治网络违法犯罪，组织网络安全攻关，宣传网络安全技能，营造网络安全环境。正如美国未来学家托夫勒宣称的那样：未来“谁掌握了信息、控制了网络，谁就将拥有整个世界”。为此，我们站在军事、战争、作战的角度来谈信息对抗、黑客攻防和网络安全。

网络空间作战是指敌对双方在网络空间所进行的一系列感知、攻防、追踪、支援和指挥与控制的战术技术行动。美国空军曾发布一份报告，预测到 2025 年，大部分战争可能不是攻击本土，甚至不发生在地球表面，而更可能发生在网络空间。美国智库兰德公司指出，工业时代的战略战是核战争，信息时代的战略战主要是网络战。目前，网络战争现实化、网络战场全球化、网络对抗常态化、网络攻心白热化的趋势明显。网络空间作战能使得武器系统出现故障、失控或爆炸，能使飞机坠毁，让军队进入埋伏区，让导弹发射到错误地区，使金融系统崩溃，使作战体系陷入指挥失灵、协同失调的严重不利

局面。网络空间一旦遭到攻击并被摧毁，整个军队的战斗力会降低甚至丧失，军事机器就会处于瘫痪状态。通过网络空间对敌实施精确、高效打击，能起到发现即摧毁的秒杀、精打巧夺、“四两拨千斤”的作用。网络空间作战正逐渐撑起战争胜负的“大旗”，正在成为一种全新的作战理念，“芯片比弹药的威力更大”，黑客的作用甚至能够胜过千军万马。实现国家战略安全和网络强军的目标，将越来越依赖有效的网络空间作战行动，以及对联合作战环境下网络空间作战能力的运用。认真探寻网络空间制胜机理，对于打赢未来信息化战争具有重要意义。

本书是近几年网络空间安全研究的结晶。我们从不同侧面、不同应用角度，推陈出新地编著出了这部反映时代发展水平和趋向的新一代图书。本书以网络空间敌对双方的作战行动为主线，试图梳理出一个清晰的网络空间战略脉络，展示如何构建一张安全之网，来检测、牵制并控制对手。同时，本书以实际案例的形式来对作战行动进行介绍，还列出了许多通俗易懂的图文解释步骤，按照步骤即可还原当时的作战情景，使读者能够对书中主要内容有比较深入的感性认识。这样一来，通过阅读本书，初学者便可以很快地掌握网络空间作战的流程、最新的技术和方法；有经验的读者则可以在技术上更上一层楼，对网络战术技术行动的认识从理论到实践并更加系统化，同时还可以使用本书介绍的一些防御方法加固自己的计算机系统。通过本书的学习，不仅能够帮助读者理解网络空间作战机理，从进攻中学会如何进行感知、防御和追踪，如何寻求支援，如何将网络面对的安全风险降至最低，全面提高网络安全防范意识、网络安全的水平和应对各种网络突发事件的能力，而且还能帮助读者少走弯路，快速掌握最新的网络安全技术，建立完整的网络安全体系和作战体系，学到最佳做法并规划设计中小型网络安全系统，帮助读者全面解决网络安全的问题。

本书力求在创新性、前瞻性和应用性等方面形成特色。在内容安排上力求由浅入深、循序渐进、前呼后应，用新颖、结构化的图例介绍其概念；在语言表达方面，力求通俗易懂、言简意赅，将枯燥的知识演绎得生动、有趣；在难易程度、广度与深度方面进行了综合考虑；在理论与实践、经典与现代、综合与探索、技术与技能、知识与应用的融合方面，在反映新内容、新理论、新技术、新思想、新观念和新成果方面开创了新局面；在概念、原理、技术、数据和结论的梳理方面，力求从不同的来源，多视角、多侧面进行考察、检验和论证，以确保其正确性；在总体把握上力求符合认知、自学、作战和教学规律，引导读者主动探索知识的奥秘。结合科学技术的重大进展，培养读者的创新思维和创新意识；通过对常见的安全场景中解决方案的讲解，帮助读者全面掌握各种作战和实用技能。

本书基本涵盖了当前网络空间作战及其应用的方方面面。首先从理论角度对网络空间及其作战的作用、影响、概念、特点、要求、组成、关系、环境和过程进行了详尽的介绍。以独特的视角、全球视野和国家维度，从现实威胁和战略高度，披露了世界各国，特别是美国的网络空间作战态势、作战力量、指挥控制、演习训练和选人用人机制，分析了各国在网络空间的国家战略和生死较量，揭示了以美国为首的西方国家正在网络空间发起新一轮攻势。回答了如何全面、正确地认识、把握与利用各种网络空间心理战武



器、态势感知与支援武器、进攻与防御武器，如何设计和规划网络靶场等方面的问题。详细剖析了网络空间态势感知的主要技术、手段、模型、组成、架构、评估、预警及系统设计；进攻手段和战法；防御的预防手段和响应手段；进攻源追踪的结构、流程和技术；指挥与控制的思想、原则、方式、关系、流程、战技、组构、编成、体制机制。综合阐述了网络空间作战的来龙去脉、基本原理、运行机制、实现方法、制胜谋略、规划部署、优化模型和行动方案；提出了各种应对策略、建议和完整的解决思路和技术途径。

本书正是为广大的网络空间安全及作战的爱好者与工作者、渴望新技术知识的人们、网络工程师、保障数据安全的日常办公人员、地方政府和军队的管理与参战及指挥决策人员、科研机构的研究人员和大学师生而写的，也可供从事武器装备论证、评估的科技人员及作战部队进行系统分析和决策时参考。希望读者通过阅读本书就能掌握网络空间作战的基本内容和新技术，更希望此书能成为读者学习的向导、工具和良师益友，在系统、全面、深入地掌握网络空间作战的机理与筹划时起到抛砖引玉的作用，进一步培养分析问题和解决问题的能力，为今后的学习和研究奠定基础。本书将为读者打开一扇通往未来的窗户，帮助读者拓宽视野，完善知识结构，储备适用于未来发展需要的知识和技能。相信读者经过本书的阅读，一定会获得精神的愉悦和智慧的启迪，一定会对网络空间作战有一个全面而深入的了解，从而真正指导作战与实践工作，使读者真正有所收获。

本书由敖志刚编著，参加部分编写工作的还有高健、敖天鸾、赵振南、童俊、朱燕飞、康兴挡、陈维鹏、吴海平、王真军、王冠、陈康、唐长春、张康益、王有成和毕衡光。吴迎（敖志刚的爱人）为本书付出了许多辛勤的汗水和劳动；陆军工程大学机关和工程保障信息化教研中心的领导和同事们给予了许多关爱、支持和帮助；电子工业出版社给予了大力协助和关怀，尤其是编辑李树林老师做了大量的工作。借此机会向他们表示衷心的感谢和敬意。

在编撰过程中，尽管我们精益求精，但由于编著者的理论水平和时间所限，对许多新技术的理解尚欠深入，书中可能会有错误与不妥之处，恳请广大读者批评指正。

编著者  
2018年8月



# 目 录

第 1 章 网络空间及其作战问题	1
1.1 网络空间的作用与影响	1
1.1.1 网络空间的应用场景和作用	1
1.1.2 网络空间对国家安全的影响	4
1.2 网络空间的概念、组成与特点	9
1.2.1 网络空间的起源	9
1.2.2 网络空间的基本概念及其架构	10
1.2.3 网络空间的组成	13
1.2.4 网络空间的特点	14
1.3 网络空间作战的内容特征和能力要求	18
1.3.1 网络空间作战的概念和相关问题	18
1.3.2 网络空间作战的本质特征	22
1.3.3 网络空间作战的内容形式	24
1.3.4 网络空间作战能力要求	31
1.4 网络空间作战环境与作战流程	32
1.4.1 网络空间作战环境	32
1.4.2 网络空间战场的组成	34
1.4.3 网络空间作战的过程	36
1.5 网络空间作战与其他作战之间的关系	38
1.5.1 网络空间作战与电子战的关系	38
1.5.2 网络空间作战与网络战之间的关系	40
1.5.3 网络空间作战与信息作战之间的关系	41
1.5.4 网络空间作战与机动作战、火力作战之间的关系	42

第 2 章 美国网络空间作战战略和指挥控制体系	43
2.1 美国网络空间作战战略分析	43
2.1.1 美国网络空间的战略基础	43
2.1.2 美国的国家战略重点	45
2.1.3 美国网络空间的全球战略	48
2.2 美国网络空间作战基本政策和策略的制定	49
2.2.1 国家信息基础设施的全面建设行动计划与重点防御战略的制定	49
2.2.2 攻防兼备, 确保网络空间安全的国家战略的制定	51
2.2.3 先发制人, 加强争夺网络空间霸权的政策和策略的制定	54
2.3 美国网络空间作战力量及其指挥控制机制	59
2.3.1 美国国家层面上的网络安全机构	59
2.3.2 美军指挥控制链	61
2.3.3 国防部组建的网络空间作战指挥机构及其职能	62
2.3.4 美军网络空间作战指挥与控制的关系	64
2.3.5 美国网络司令部的工作重点和使命任务	66
2.4 美国陆军网络空间作战力量和指挥控制体系	68
2.4.1 美国陆军网络空间作战机构及职能分工	68
2.4.2 陆军网络空间作战指挥与控制关系	71
2.5 美国空军网络空间作战力量和指挥控制体系	72
2.5.1 空军网络空间作战的组建过程	72
2.5.2 空军网络空间作战的指挥关系和使命任务	75
2.6 美国海军网络空间作战力量和指挥控制体系	78
2.6.1 海军网络空间作战力量的组建	78
2.6.2 海军舰队网络空间作战主要机构的职责、使命任务和指挥关系	79
2.6.3 海军舰队全球网络作战指挥与控制	82
2.6.4 海军陆战队网络空间作战的目的、职责和任务	83
2.6.5 海军陆战队网络作战指挥的管理流程	84
2.6.6 海军陆战队网络作战组织机构	84
2.7 美军网络空间作战人才的选拔、培养与模拟训练	86
2.7.1 美军网络空间作战人才的选拔	86
2.7.2 美军网络空间作战人才的培养和训练	88
2.8 美军网络空间作战演习	90
2.8.1 “网络风暴”演习	90
2.8.2 “网络防御”演习	96

2.8.3	“网络闪电”演习	101
2.8.4	“施里弗”太空演习	102
2.8.5	“网络卫士”演习	103
2.8.6	美军其他网络空间作战演习	107
<b>第3章</b>	<b>网络空间作战武器</b>	<b>111</b>
3.1	网络空间作战武器基本内容	111
3.1.1	概念与特征	111
3.1.2	主要对象、任务和目标	112
3.1.3	网络空间作战武器的能力体系	113
3.1.4	网络空间作战武器的分类	115
3.1.5	网络空间作战武器的作用	117
3.1.6	网络空间作战武器的发展趋势	119
3.2	网络空间心理战武器	120
3.2.1	网络空间心理战的概念与特点	121
3.2.2	网络空间心理战对抗模型和武器体系	123
3.2.3	网络空间心理战的主要手段	125
3.2.4	网络空间心理战典型的几种武器	127
3.3	网络空间态势感知武器	131
3.3.1	网络扫描器	132
3.3.2	网络监听器与工具	135
3.3.3	网络密码破译器	137
3.3.4	电磁侦测器	139
3.3.5	“爱因斯坦”计划	140
3.3.6	网络入侵检测系统	146
3.3.7	网络飞机	148
3.3.8	其他态势感知武器	152
3.4	网络空间进攻武器	152
3.4.1	网络空间进攻武器的分类	152
3.4.2	常用的网络空间进攻武器	154
3.4.3	舒特系统武器	160
3.4.4	震网病毒武器	164
3.4.5	数字大炮	167
3.4.6	下一代干扰机	170
3.4.7	高功率微波武器	173
3.5	网络空间防御武器	180

3.5.1	网络空间常用的防御武器	180
3.5.2	网络诱骗系统	184
3.5.3	网络攻击预警系统	190
3.5.4	其他的防御武器简介	194
3.6	网络空间支援武器	195
3.6.1	网络空间的漏洞评估	195
3.6.2	网络空间安全态势的评估	200
第4章	网络靶场规划及其建设	207
4.1	概述	207
4.1.1	建设网络靶场的必要性	207
4.1.2	网络靶场的概念	209
4.1.3	网络靶场的特点	210
4.1.4	网络靶场的任务与目标	212
4.1.5	网络靶场的功能需求分析	214
4.1.6	网络靶场国内外研究现状	215
4.2	网络靶场的设计与规划	217
4.2.1	网络靶场的设计要素与架构	217
4.2.2	网络靶场的系统实现	219
4.2.3	国家网络靶场系统设计架构及与传统靶场的比较	222
4.2.4	网络靶场核心技术	224
4.2.5	网络靶场能力体系	226
4.3	美国国家网络靶场的规划与建设	228
4.3.1	远景、目标和功能	229
4.3.2	实施计划与任务	231
4.3.3	建设方案	235
4.3.4	试验特点与流程	238
4.3.5	网络靶场能力发展思路及体系框架分析	240
4.3.6	使用的最新技术和方法	242
4.4	美国几种典型的网络靶场的建设情况	243
4.4.1	国防部信息确保靶场	243
4.4.2	联合网络空间作战靶场	245
4.4.3	海军网络靶场建设思路	246
4.4.4	联合信息作战靶场	250
4.4.5	美军网络靶场建设发展特点	251

第 5 章 网络空间作战态势感知	253
5.1 基本概念与知识	253
5.1.1 网络空间态势感知的内涵	253
5.1.2 态势感知技术分类	257
5.1.3 网络空间作战态势感知的目的、原则与任务	259
5.2 网络空间作战态势感知的主要技术	261
5.2.1 入侵检测技术	261
5.2.2 信息融合技术	264
5.2.3 数据挖掘技术	265
5.2.4 信息可视化技术	270
5.2.5 恶意代码检测技术	273
5.2.6 风险分析与评估技术	274
5.3 网络空间态势感知的主要手段	275
5.3.1 网络扫描技术及其算法	276
5.3.2 网络侦听	280
5.3.3 密码破译	281
5.3.4 介质窃密	282
5.4 网络空间作战态势感知模型	283
5.4.1 网络空间态势感知的分析模型	283
5.4.2 网络空间作战态势感知的功能模型	284
5.4.3 网络空间层次化态势感知模型	287
5.4.4 可视化态势感知模型	288
5.5 网络空间作战态势感知的体系结构及其组成	289
5.5.1 体系结构	289
5.5.2 态势感知系统分析架构	291
5.5.3 态势感知支撑平台的组成	293
5.6 网络空间作战态势感知系统的设计	296
5.6.1 设计原则和目标	296
5.6.2 系统功能需求分析	297
5.6.3 网络空间作战态势感知系统总体架构的设计	299
5.6.4 信息获取层的设计	300
5.6.5 要素提取层的设计	301
5.6.6 态势决策层的设计	303
5.6.7 系统部署架构	304

5.7 网络空间作战态势感知的评估 .....	305
5.7.1 网络空间作战态势感知的评估过程 .....	305
5.7.2 网络态势评估系统体系架构 .....	307
5.7.3 态势评价指标选取 .....	310
5.8 网络空间作战态势感知的预警 .....	313
5.8.1 概念与目的 .....	313
5.8.2 预警系统的组成 .....	314
5.8.3 预警系统的结构 .....	314
5.8.4 预警系统的工作流程 .....	316
5.8.5 态势预测子系统功能描述 .....	317
<b>第 6 章 进攻性网络空间作战 .....</b>	<b>321</b>
6.1 概述 .....	321
6.1.1 进攻性网络空间作战的目的 .....	321
6.1.2 网络空间进攻作战的原则 .....	322
6.1.3 进攻性网络空间作战的分类 .....	324
6.1.4 网络空间进攻的流程 .....	327
6.1.5 网络空间进攻性作战机理 .....	330
6.2 网络空间进攻的主要手段 .....	334
6.2.1 计算机病毒攻击 .....	334
6.2.2 欺骗类攻击 .....	339
6.2.3 拒绝服务攻击 .....	344
6.2.4 口令攻击 .....	350
6.2.5 缓冲区溢出攻击 .....	353
6.2.6 Web 攻击 .....	357
6.2.7 密码分析攻击 .....	361
6.3 网络空间进攻中的作战战法 .....	363
6.3.1 网络空间进攻作战的主要模式 .....	363
6.3.2 网络空间舆论进攻战法 .....	364
6.3.3 网络虚拟战法 .....	367
6.3.4 以奇制敌取胜战法 .....	369
6.3.5 破“墙”击要法 .....	370
6.3.6 毁“网”断流法 .....	371
6.3.7 夺“点”控网法 .....	372
6.3.8 断“源”瘫网法 .....	372
6.3.9 先“动”后“静”法 .....	372



6.3.10	局部造优法 .....	373
6.3.11	网电一体进攻战法 .....	373
6.3.12	网络空间进攻的实施方法 .....	376
<b>第 7 章</b>	<b>防御性网络空间作战 .....</b>	<b>379</b>
7.1	网络空间作战防御基础 .....	379
7.1.1	网络空间作战防御的概念与分类 .....	379
7.1.2	网络空间安全防御系统的功能体系 .....	381
7.1.3	网络信息安全防御的基本属性与机制 .....	381
7.1.4	网络信息安全等级保护的法律法规和政策标准 .....	385
7.1.5	网络空间信息防御体系的层次结构 .....	390
7.1.6	网络空间信息防御的体系结构 .....	392
7.1.7	网络空间安全防御过程 .....	394
7.1.8	网络安全防范体系设计准则 .....	395
7.2	网络空间作战的预防手段 .....	396
7.2.1	防火墙技术 .....	396
7.2.2	防病毒技术 .....	402
7.2.3	数据加密技术 .....	406
7.2.4	信息隐藏技术 .....	410
7.2.5	访问控制技术 .....	413
7.3	网络空间作战防御的响应手段 .....	418
7.3.1	欺骗类攻击的防御 .....	418
7.3.2	拒绝服务攻击的防御 .....	422
7.3.3	口令攻击的防御 .....	427
7.3.4	缓冲区溢出的防御 .....	429
7.3.5	Web 攻击的防御 .....	434
7.3.6	数据恢复技术手段 .....	439
<b>第 8 章</b>	<b>网络空间进攻源的追踪 .....</b>	<b>443</b>
8.1	网络空间作战进攻源追踪概述 .....	443
8.1.1	网络空间进攻源追踪的概念与作用 .....	443
8.1.2	网络空间进攻源追踪的困难与面临的挑战 .....	444
8.1.3	网络空间进攻源追踪的分类 .....	447
8.1.4	网络进攻源追踪的信息及其获取 .....	451
8.1.5	进攻源追踪机制的性能评价指标 .....	455
8.2	网络空间进攻源追踪的运行机制 .....	456
8.2.1	网络空间进攻源追踪的一般过程 .....	456

8.2.2	系统组件及其功能	458
8.2.3	网络空间进攻源追踪的系统原理	460
8.3	网络空间进攻源追踪的体系结构	463
8.3.1	分布式和集中式拓扑结构	463
8.3.2	一种通用网络追踪技术框架	464
8.3.3	网络空间黑客追踪的系统结构	465
8.3.4	网络空间多源追踪系统架构	467
8.3.5	网络空间主动追踪机制体系结构	469
8.4	网络空间 IP 源追踪技术	472
8.4.1	数据包标记法	472
8.4.2	路由记录法	478
8.4.3	ICMP 消息法	480
8.4.4	入口过滤法	482
8.4.5	链路测试法	485
8.4.6	层叠网络追踪	488
8.4.7	IP 源追踪技术的比较	489
8.4.8	IP 源追踪面临的关键问题与研究展望	490
8.5	面向连接链的追踪技术	492
8.5.1	基于网络的连接链追踪技术	492
8.5.2	基于主机的连接链追踪技术	495
8.5.3	基于主动网络的连接链追踪技术	497
8.5.4	面向连接链追踪技术的性能比较	500
第 9 章	网络空间作战的指挥控制	503
9.1	联合作战下的指挥控制	503
9.1.1	基本概念与内涵	503
9.1.2	指挥控制过程	506
9.1.3	指挥控制的系统架构	508
9.2	网络空间作战指挥控制的战术技术要求	510
9.2.1	网络空间作战指挥控制的基本概念与属性	510
9.2.2	网络空间作战指挥控制的特点	511
9.2.3	网络空间作战的指导思想和原则	514
9.2.4	网络空间作战指挥方式	517
9.2.5	网络空间作战指挥关系	520
9.2.6	网络空间作战指挥控制流程	521
9.2.7	网络空间作战指挥控制系统技术体系	522

9.3 网络空间作战指挥控制的体制机制 .....	524
9.3.1 网络空间作战指挥控制体系构建要求 .....	524
9.3.2 网络空间作战指挥能力构成框架与影响要素 .....	525
9.3.3 网络空间作战指挥体系的设想架构 .....	528
9.3.4 网络空间作战指挥中心的组构 .....	529
9.3.5 网络空间作战的组织结构设想方案 .....	531
9.3.6 网络空间作战力量的编成考虑 .....	533
附录 英文缩略语及其中英文对照 .....	535
参考文献 .....	539



# 第 1 章

## 网络空间及其作战问题

自古以来，围绕争夺生存活动空间的斗争从未中断过，从热衷陆地占领，到追求海空控制，再到太空角逐、实施电磁压制，人类在空间博弈的漫长过程中，不仅拓展了控制空间的能力，还形成了夺取空间制权理论。与之如影相随的是，国家安全的边界也从有形的地理边疆，拓展到无形的网络电磁空间。网络空间安全已经上升为信息化条件下国家安全的一项核心内容。社会越进步，经济越发展，人类活动对网络空间的依赖性越大，网络空间安全对国家安全的影响就越突出。今天，利用电子、光子和电磁频谱进行信息获取、传输、交换、处理和共享，已经成为时代的标志之一。保护国家关键信息基础设施、应对信息时代网络空间安全威胁、实现国家战略安全目标，将越来越依赖有效的网络空间作战行动，以及对联合作战环境下网络空间作战能力的运用。

### 1.1 网络空间的作用与影响

#### 1.1.1 网络空间的应用场景和作用

德国哲学家海德格尔指出，人的存在决定了世界的存在。人“在世界之中”的存在方

式决定了人生活的世界的存在。人们在互联网之中的学习、工作、休闲、购物等都发生“在网络之中”。所以从海德格尔的空间观念来说，人“在网络之中”的存在方式决定了一个新型人类生活空间的显现和存在。这个空间就是网络空间（Cyberspace）。如今网络空间正在以一种不可逆转的趋势渗透进我们的生活，改变着我们的生活方式，塑造着一种前所未有的人类生活和未来。

信息时代，网络空间已经开始向世界各个角落辐射，政治、经济、军事、文化领域无不渗透着网络的身影。网络空间的主要部分是互联网，互联网是人类的共同家园。据《中国互联网络发展状况统计报告》显示，截至2016年12月，中国网民规模达7.31亿，互联网普及率达到53.2%，其中，2016年新增网民4299万，增长率为6.2%；我国手机网民规模达6.95亿，手机网上支付用户规模为4.69亿；我国网站总数为482万，域名总数为4228万，网页数量2360亿。据工业和信息化部统计，到2016年年底，我国互联网宽带接入端口数量为6.9亿。全世界约一半人口使用了互联网。

网络空间通过跨国界的网络控制与应用，以及数据库、搜索引擎、电子邮箱在全球范围内进行渗透，社交网络、微信、博客、微博和短信成为信息联络与传递渠道。人们可以通过网络空间实现以往许多不可能实现的愿望，如人们坐在计算机前面敲击键盘就能够与远在异国的朋友进行信息交流，能够阅读某个大学图书馆的书籍，能够与白宫的某位官员交谈，能够与非洲的陌生人就气候问题交换意见，能够浏览BBC最新的资讯，甚至能够逛一下米兰的商店购买几件自己喜欢的时装等。不同种族、不同国家、不同文化背景的人在网络上交流思想，交换商品，获取信息，合作完成工作，甚至寻求情感慰藉。互联网已经构建了一个人们共同活动的空间，已经从一种单纯的交流工具变成人们生活和实践的一种方式。通过互联网连接，业务可以延伸至全球任何一个地方，为大众创造无以计数的就业岗位和机会；非洲的农妇可以向拉丁美洲的家庭出售手工艺品，从而实现更广阔的经济发展；欧洲的实验室可以利用亚洲生产的硬件和北美研发的软件进行开创性的研究；各个国家的学生可以通过视频会议系统共同学习；各国民众在信息技术的帮助下，可以使其政府变得更加开放和负责。

信息技术使国际货物和服务的流动更加便利。水电供应、空中管制、金融系统等维持正常生活所必需的基础设施都离不开网络化的信息系统。政府可以通过“电子政务”向民众提供基本的服务。社会和政治运动也依赖互联网形成新的、影响力更大的组织和行动。网络化的技术在全球无处不在。

对个人来说，计算机网络已经提高了生产力，促进了经济繁荣，帮助解决了各类缺陷和不足，融合了因语言或疾病而造成的隔离，并使身处偏远贫瘠地区的家庭和亲友建立联系。对社区来说，它提升了应对突发事件的能力，扩大了信息共享以打击犯罪，曝光腐败行为，为政治活动提供了便利条件，从而能够关注被忽视的议题。对商业来说，它开拓了市场，培育了价值数十亿美元的产业。对政府来说，它增强了决策透明度，提高了工作效率，增加了便利，并使领导人与其服务的民众之间得以联系和沟通。对国家来说，网络空间的开发和利用，促进了信息基础设施建设、科学研究、新兴技术与产业的发展，提升了综合国力；对国际社会来说，网络空间的博弈与争夺，提供了一个新的全球思想市场，造

成国家间力量的相对上升或下降，为应对灾难提供了更加便利的解决渠道，由此塑造新的国际格局。信息流通越自由，我们的社会就越牢固。若运用得当，这些技术将全面增强我们的力量，将进一步拓展网络技术的应用领域。

数字基础设施日益成为支撑繁荣的经济、活跃的研究团体、强大的军队、透明的政府和自由的社会的基础，与社会的稳定和发展密不可分。一些关乎国计民生的通信、电力、交通、银行等重要信息基础设施已经成为国家安全的重要战略资源，一旦这些重要的信息基础设施遭到破坏，国家将陷入瘫痪，甚至将有被颠覆的危险。如果不打击网上犯罪活动，将对世界和平构成新的威胁。美国前总统奥巴马在《网络空间政策评估》报告中把网络空间作为国家战略资产来对待，保护该基础设施将成为国家安全优先考虑的工作。

网络空间是联结陆、海、空、天等维度空间的中介和桥梁，是自然空间和技术空间的统一。在网络社会化、社会网络化的今天，网络空间正在加速演变为战略威慑与控制的新领域、意识形态领域斗争的新平台、维护经济社会稳定的新阵地、信息化局部战争的新战场，正在成为承载政治、经济、文化、外交、军事的全新空间。抢占网络空间领域的制高点，是保卫国家信息领域安全、捍卫国家网络主权、打赢未来战争的现实要求。其关键基础设施的安全问题直接影响社会稳定、国家安全、经济发展、文化传播，直接挑战社会管理、公民自由和公众权益。1996年美国空军发布一份报告，预测到2025年，大部分战争可能不是攻击本土，甚至不发生在地球表面，而更可能发生在网络空间。许多人认为，未来的国家安全和战争的胜负，将越来越取决于网络控制权，它是继制陆权、制海权、制空权和制天权之后的一种新权力方式。要拥有网络空间优势就必须在整个电磁频谱内实现全球警戒、全球到达和全球力量，增强精确交战、态势感知以及控制、瓦解、削弱或消除敌人在进攻方面的能力。正如美国未来学家托夫勒宣称的那样：未来“谁掌握了信息、控制了网络，谁就将拥有整个世界”。

革命性技术的出现使得网络空间能力大幅提升，并使其产生了对作战前所未有的影响。因为网络空间关系到未来军队建设与发展方向，关系到军队战斗力的高低、军事机器能否正常运行和是否能打赢，关系到国家安危与存亡，是未来战争的重要领域和行动空间，是指挥控制部队的基本依托，是联合作战体系的重要组成部分，是在战略、战役以及战术各级采取有效行动的基础，是我军信息化建设和作战必须高度关注的重大问题和领域。它将会给未来作战理念、样式和行动、建军方向带来前所未有的冲击、挑战和机遇。美国智库兰德公司指出，工业时代的战略战是核战争，信息时代的战略战主要是网络战。

网络空间作战提供了一种相对轻松就能给敌人造成巨大破坏的作战方式。这是一场高技术作战和战略战，它能使得武器系统出现故障、停止工作或出现爆炸，能让火车脱轨，使飞机坠毁，让军队进入埋伏区，让导弹发射到错误地区，使金融系统崩溃、供应链停止、卫星脱离轨道、航班停飞。网络空间一旦遭到攻击并被摧毁，整个军队的战斗力会降低甚至丧失，军事机器就会处于瘫痪状态。谁能够抢先夺取网络空间的战略制高点，就意味着谁将掌控体系与体系对抗的主动权。

在未来网络空间战场上，“芯片比弹药的威力更大”，黑客的作用甚至能够胜过千军万马。保护网络空间是一项要求所有人都积极参与的复杂事业。

## 1.1.2 网络空间对国家安全的影响

由于信息社会的特殊属性，网络空间实际上为在技术上拥有优势地位的大国提供了影响和控制实体领域的新手段，如今已经深刻地影响着政府的运作方式、军队的作战方式、企业的经营方式和人们的生活方式等方方面面，同时也对国家安全的各个层面产生影响。

### 1. 对国家政治安全的影响

政治安全是国家安全的核心部分，是指一个国家有效地防范来自国内外的政治干预、压力和颠覆以及敌对分子的破坏活动，从而确保国家主权独立、领土完整、政权稳定等的良好运行状态。网络空间及其安全对国家政治安全的影响主要表现在以下几个方面：

首先，网络空间的出现使得国家主权相对弱化。正如未来学家约翰·奈斯比特所说：“信息革命使国家淡化了，这是由于世界已没有界限。但是由什么来取代国家？它们正在被网络所取代。”网络空间的出现使得国家主权的外延从领海、领空扩大到“信息边疆”。由于网络空间本身的物理特性即开放性，使它突破了传统地理距离的空间限制。这冲击了传统的封闭性的主权理论，并产生了“信息主权”。由于信息网络分布广泛，几乎遍及世界的任何一个角落，从而导致频繁越境的跨国信息流突破了地理空间的局限。信息网络的出现使得一个人远在千里之外就可以轻易地实施自己的意图，使得思维与实践相“分离”，这会大大削弱国家对信息的控制权和管理权。没有信息主权的安全，就不可能有国家真正的安全。维护信息主权的安全，正在成为维护国家主权完整的核心内容之一。信息网络的发展使得国际组织、跨国公司、特殊利益集团，以及非国家行为体，甚至个人等国际政治新兴行为体能够得以依托，从而进一步参与国际活动，发挥更大的作用，这在一定程度上弱化了国家在国际政治中的地位。

其次，数字鸿沟的出现。由于在客观上各个国家所发展的信息技术的差异性普遍存在的，这使得在信息技术方面具有优势的国家在一定程度上就拥有了对信息网络的相对控制权。其对关键信息技术垄断的行为，阻碍了发展中国家和不发达国家在信息技术领域的发展，在一定程度上扩大了国家地位事实上的不平等。如今在发达国家与发展中国家之间的信息技术开发和使用方面的差距不断加大，从而加深加剧了发展中国家自身的政治、经济、军事、文化和社会问题，形成了信息时代的“马太效应”。大国依然拥有更加雄厚的资源，在互联网中，并非所有的行为者都是平等的。

第三，网络空间成为异己分子进行敌对行动的新媒介。信息网络的开放和便利，为一些异己分子和组织宣扬歪理邪说扩散政治影响提供了可乘之机。他们利用网络散布谣言蓄意挑起事端、攻击国家信息基础设施引发国家政局不稳，人民生活不安宁，他们暗地招募恐怖分子进行恐怖主义活动，给国家的政治稳定带来了不利影响。

第四，网络权力的产生。借助于网络空间这个平台使得信息技术等为核心的信息技术革命得以在全世界范围内推进，使传统上的权力的概念也发生了变化。哈佛大学教授约瑟夫·奈认为权力可以分为软权力和硬权力。软权力是指吸引力权力，包括国家凝聚力、文



化吸引力、价值观和政治制度的吸引力，以及创设国际机制的能力。硬权力是指支配性权力，诸如军事实力、经济实力和科技实力等。他认为在信息时代，软权力正变得比以往任何时候更有影响力。网络权力能够在网络空间内部产生希望得到的结果，其作用也可以延伸到网络领域之外的其他领域。

相较于许多其他传统权力领域而言，成本投入低廉、允许匿名操作、脆弱性以及不对称性等特征，意味着非国家行为者在网络空间能够行使更多的硬权力和软权力。网络空间是一个比较活跃的新型人造环境，网络空间自身具备的某些特点能够降低行为者之间权力差异，从而能够使权力扩散。信息领域的变革总是能够对权力产生重要影响，显然世界的权力格局、增长和发展模式、竞争与威胁战略、社会控制和智力结构等诸多方面都出现了新的维度和趋势，但同时也带来了许多新的挑战。

## 2. 对国家经济安全的影响

在国家安全之中，经济安全占有十分重要的地位。随着信息网络技术在经济领域的广泛应用，网络空间逐渐成为经济活动的主要场所，其信息技术和信息产业正在成为世界经济的主要推动力量和新的增长方式。金融活动信息化和电子货币在电子商务中的广泛普及说明信息已经成为经济活动的资本、支付手段和贸易手段。人们在进行贸易往来的时候只需轻轻敲打几下键盘就能完成所需的经济活动。贸易过程已经表现为信息的传输、流动和转换。现在，借助计算机网络就可以在世界任何地方调动全球金融资源，无论发达国家还是发展中国家，国际资本通过信息网络进行大规模的交易活动已经随处可见。

目前，网络空间对国家经济安全的影响主要表现在以下两个方面：

一是信息基础设施本身的脆弱性给国家经济安全带来影响。在过去的半个世纪中，全球一体化明显地加速了，越来越多的国家和地区融入国际经济体系中来，可是在许多方面仍然非常脆弱，容易遭到破坏，而且脆弱性在日益提高，其原因就是今天的国际经济体系依赖于一系列的互相联系的关键基础设施，而这些基础设施其范围大多远远超出了国界，并且受控于日益精巧的信息网。

二是屡屡发生网络犯罪行为给国家经济造成影响。全球化和信息网络技术的飞速发展使世界各国相互依存，加速了跨国贸易、资本的国际流动以及信息的跨国传播，人员、资源、技术等进行跨国优化组合和资源的重新配置。在全球化的大背景下，世界各国的经济逐步形成了相互依存、紧密联系的有机整体。但经济犯罪行为也借助网络空间的平台呈现出跨地域、跨行业的特征。

目前，网络空间的许多威胁都是受个人经济利益的驱动，或者与故意破坏公共或他人的信息安全相关的。网络空间内的罪犯和犯罪企业已经越来越组织化，形成了高度组织化的个人信息、信用卡、身份和其他有价值信息的流动环。许多时候，罪犯和犯罪企业的软件和硬件的发展能力可匹敌于工业领导者发展的软件和硬件能力。当前维护全球经济安全已经成为国际社会共同面临的重大课题。

### 3. 对国家军事安全的影响

(1) 网络空间成为军备竞赛的新领域。目前，以网络技术为核心的信息技术在军事领域的广泛应用，推动了军队的新军事变革，使战争领域外延到网络空间。由于网络信息技术已经深入到社会各个领域，使得网络空间正在成为新一轮军备竞赛的新领域。早在 20 世纪 70 年代末，苏联海军司令瑟奇·格什科夫（Sergei Gorchakov）曾下过著名的论断：“能够充分利用电磁频谱的国家将赢得下一场战争。”为了取得这一“新”的作战空间的作战优势和控制权，世界各个国家竞相开展相关领域的作战研究，网络军备竞赛已经开始。美军在 2001 年的《四年防务评估报告》中认为，军事竞赛向网络空间拓展是军事技术发展的一大重要趋势。在 2010 年的《四年防务评估报告》中，将“网络空间”与“非正规作战”“战区空运”和“无人机”并列为优先发展的四大重点领域，认为网络空间是陆、海、空、天、电等领域实施指挥、控制、通信、情报、监视和侦察活动的媒介，也是美军建立和运用各种力量，有效实施战略、战役、战术层次行动的基础，是必须争夺的“新边疆”。

(2) 网络空间加速推动了新军事变革的进程。空权论的倡导者、意大利著名的军事理论家杜黑说过：“胜利总是向那些能遇见战争特性变化的人微笑，而不是向那些等待变化后才去适应的人微笑。”当今，信息网络技术的迅猛发展正在推动军事领域的重大变革，使战争形态和作战样式向信息化战争的方向发展。恩格斯曾经指出：“一旦技术上的进步可以用于军事目的并且已经用于军事目的，它们便立刻几乎强制地，而且往往是违反指挥官的意志而引起作战方式上的改变甚至变革。”在信息时代，军队的指挥控制、情报和后勤补给活动，以及武器技术的开发生产都严重依赖于信息网络，而如果没有牢固可靠的信息和通信网络保障，没有网络空间的支持，仅靠现代化武装部队自身是无法执行快节奏、高效率的作战行动的。美国海军军事战略专家约翰·阿尔奎拉认为：“世界已进入信息时代，如果我们的军队无法实现根本性转变，向更加小型化、灵巧化和高度网络化的方向发展，美国必将陷入十分尴尬的境地：耗费巨额开支，却无法打败敌人。”

(3) 破坏指挥信息系统，影响指挥决策。战时指挥信息系统一旦被敌方通过各种途径侵入并修改，将虚拟现实成果技术植入指挥控制信息系统中，将其假情报、假决策、假部署传输给己方，诱导判断失误；向官兵发布假命令、假指示、假计划，屏蔽或欺骗己方情报系统，以改变作战意图，影响高层的智慧决策。一旦敌方阴谋得逞，会干扰指挥机关的指挥控制行动，使其陷入处理各种复杂信息的事务性工作中，不能集中精力处理有关作战的重大问题，影响并削弱指挥作战，使在战略战术上不能占据有利态势，甚至直接影响到整个战役的成败。

(4) 渗透军事信息网络，获取军事情报。网络空间作战大大拓宽了情报的获取方法和渠道，敌方可通过破解对方程序密码，直接或间接进入军事信息网络或军用计算机，获取军事斗争决策、军事力量部署、装备性能参数等军事情报，造成极大损失。同时，由于可以对所窃取的信息进行加密，掩盖痕迹，对方将无法及时察觉网络攻击行动。更有甚者，将永远无法获知敌方窃取了哪些机密信息，造成的后果是无法想象的。2008 年的下半年，

美国证实了“一次非法入侵机密网络：通过某个受病毒感染的指纹驱动器，入侵到监控伊拉克和阿富汗战争的中央指挥系统中，足足一个星期后入侵者才被剔除，且没人知道这次入侵导致的损失究竟有多大。

(5) 侵入武器控制网络，削弱作战能力。近年来，随着武器装备的不断更新，自动化程度越来越高，很多武器控制系统由计算机智能控制，如果敌方侵入武器控制网络或通过控制带有“预设”后门的计算机、数字信号处理器、大规模集成电路的武器装备，使武器系统按照敌方意图操作或因程序错误而发生自行爆炸、自我摧毁以及相互残杀等，达到摧毁武器平台、削弱作战能力的目的。2011年，美军RQ—170无人侦察机被伊朗俘获，坠落原因有一种可能就是被伊朗网络空间作战部队控制并操控其坠落境内。

(6) 瘫痪空防作战系统，降低作战效能。敌方可利用空防作战系统的网络“后门”漏洞，将网络病毒或分布式拒绝服务等工具远程植入或无线注入空防作战系统，在关键时刻使病毒发作，侵害系统软件，使整个系统瘫痪。通过“破网”，破击战场信息网络，瘫痪指挥信息系统和信息基础设施，降低情报支援能力和战场信息情报感知能力，使作战力量难以有效聚合，从而使整个空防体系要素分离、功能分散、结构坍塌，难以实施有效作战。

有学者曾说，在信息时代，一枚核弹的作用，或许不敌一名黑客。“如果你对一幢房屋投掷一枚炸弹，我们可以十分清楚地了解其直接与间接损害有多大。如果你进入并瘫痪某个地方，特别是涉及国家安全的服务器，我们就很难清楚可能的后果。”美国军事专家詹姆斯·亚当斯在其所著的《下一场战争》中曾预言，未来战争中“夺取作战空间控制权的将不是炮弹和子弹，而是计算机网络里流动的比特和字节”。冷战时期，使用战机越洋攻击需要数个小时；冷战后，使用导弹越洋攻击需要几十分钟；而现在从某种意义上来说，网络空间可以以电子的速度进行运转，一个相对简单的信息攻击能够以发送一封电子邮件所花费的相同的时间来完成。网络空间已成为决胜千里之外的高速战场。

#### 4. 对国家文化安全的影响

文化安全，是指一国在文化、精神生活方面不受外来文化的干扰、控制和同化，从而保持本民族的价值观念、生活方式的民族性以及本国意识形态的自主性。文化安全是国家安全的重要组成部分，对于以文化为精神凝结手段的国家来说，确保本国文化的安全是维持其国家稳定的基础，也是其生存和发展的基本前提。国家文化安全通常包括语言文字的安全、风俗习惯的安全、价值观念的安全和生活方式的安全等内容。随着信息网络技术的不断发展，网络空间作为全球开放的文化共享和传播平台，打破了传统的文化传播模式，对文化发展、创新、传播和管理都产生了深远的影响。但同时，信息网络技术的发展推动了全球化的深入发展，也带来了信息传播模式的重大变化，在加速文化传播和交流的同时，也导致了“文化霸权主义”“文化殖民主义”甚至“文化帝国主义”的出现。从某种程度上来说，国家文化安全就是国家进行“反霸权”“反殖民”“反帝国主义”的文化战略。

西方一些发达国家凭借自己掌握的信息优势对媒体进行操控，对其他国家倾销其文化和价值观。这使一些国家传统文化面临着被“边缘化”的危险，使国家的文化安全在信息时代面临着非常严峻的挑战。在科学技术日益进步的今天，互联网的发展使国家行使主权

的能力受到制约，国家再也不能以绝对的权威控制信息的传播，干预国际间的交流。美国中央情报局声称：“我们要利用一切手段来毁灭他们的道德人心，摧毁他们的自尊自信心，尽量打击他们刻苦耐劳的精神。”美国认为，“在新世界，自由将通过移动电话和因特网传播”。某些被发达国家所掌控的国际组织，在某种程度上也扮演了推行西方价值观的角色。很多与文化领域相关的国际组织，受到一些发达国家的操控，往往有计划有组织地推进各国间的文化交流活动，在增进各国间相互了解的同时，甚至在向不发达国家提供援助时也不忘记推销其价值观和所谓的道德规范。这些都会让国家主权内的文化自主性受到冲击。

## 5. 关键基础设施的安全问题直接影响到社会稳定与经济发展

现代社会强烈依赖大规模的国家基础设施来保障国民经济的平稳运行和公共服务的正常提供。目前，信息基础设施已经具有与电力基础设施同等的重要地位，并成为连接其他各个基础设施部门的关键纽带；信息基础设施的正常稳定运转为政府、金融、能源、交通运输、公共卫生、供水和应急服务等与国计民生密切相关的重要系统，以及政府事务管理提供关键支撑。我国相互依存的关键基础设施模型如图 1-1 所示。因此，国家网络空间的安全与否将直接影响国家的社会稳定与经济发展。

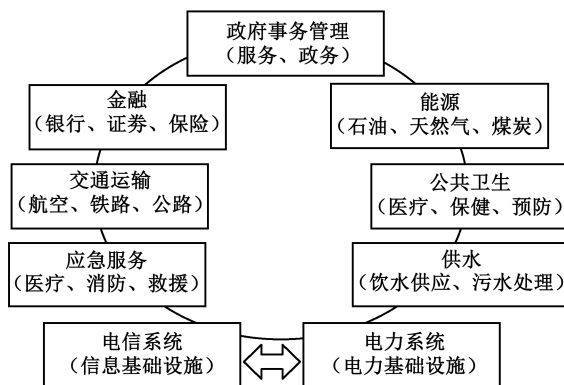


图 1-1 我国相互依存的关键基础设施模型

## 6. 网络空间已经成为东西方主流意识形态对抗的主战场

全球一体的互联网平台使得网络信息传播表现出明显的跨国性特点。国家对信息传播的垄断权力受到极大限制，对内的最高性和对外的独立性呈现相对化趋势。正基于此，网络霸权国家利用其优势的制信息权对外进行持续的意识形态渗透和控制。

2010 年年初“谷歌事件”之后，美国原国务卿希拉里发表了被称为“希拉里宣言”的互联网自由演讲，指出“互联网自由是美国长期推动国外民主的关键”。美国政府进而提出“信息国界是对民主的挑战、不接受任何可能妨碍信息流动的举措”的观点，将矛头直指中国并以美国宪法和“人权宣言”第 19 条来压制我国互联网管理政策和措施，英、德等国亦有呼应。

然而，希拉里与美国政府的“伪自由”谎言很快遭到了现世报。2010 年 11 月 28 日，

“维基解密”网站曝光了逾 25 万份据称是美国国防部的机密文件，显示美国外交官曾被要求监视联合国领导层和安理会常任理事国的代表们。显而易见，希拉里所谓“互联网自由”恐怕只是美国一国对全球互联网信息控制的自由。这也证明了网络传媒已经成为国家宣示主权的重要资源和对外战略的重要手段，网络空间已经成为东西方主流意识形态对抗的主战场。

## 7. 网络空间安全威胁直接挑战社会管理和公众权益

经过近些年的普及和发展，互联网已成为社会监督、通达民意和了解舆情的重要渠道，社会深层矛盾和各种利益诉求在网络空间均得以充分展现。然而，另一方面，网络舆论导向、道德伦理和意识形态的渗透和侵蚀问题也已凸现。

例如，非理性的网络舆论不但混淆真相、挑拨是非，甚至通过挟持民意而影响到司法公正；网络社区、手机短信及其他衍生信息服务平台常常被利用成为散播谣言、煽动情绪、激化矛盾和引发社会群体性事件的动员工具。

又如，搜索引擎技术的发明为信息搜集与传播提供了快速便捷的通道，使互联网因之成为侵犯个人隐私的主要平台。近年来，所谓网络追杀、网络流言、人肉搜索等网络暴力事件此起彼伏，甚至出现贩卖个人信息的黑色产业链；网络隐私保护已成为突出的社会问题。

再如，网络空间中的有害信息泛滥，其中更以淫秽色情和暴力内容为甚，严重影响缺乏自我控制能力的青少年健康人格的形成。中国预防青少年犯罪研究会的统计资料表明，目前青少年犯罪总数占全国刑事犯罪总数的 70% 以上，其中 14~18 岁的未成年人犯罪又占到青少年犯罪总数的 70% 以上，有 70% 的少年犯因受网络色情暴力内容影响而诱发盗窃、抢劫、强奸、杀人、放火等严重犯罪。

诸如此类的安全威胁，均已直接挑战政府的社会管理和公众权益，如不能有效应对，必将影响广大人民的正常生活秩序、互联网经济的整体发展和政府执政管理的公信力。

## 1.2 网络空间的概念、组成与特点

### 1.2.1 网络空间的起源

网络空间（Cyberspace），又称赛博空间，最初是由加拿大作家威廉·吉布森（William Gibson）在 1982 年所写的小说《融化的铬合金》（*Burning Chrome*）中首次使用，意思是指网络空间是由计算机所创建的虚拟信息空间。该词随着 1984 年吉布森出版的小说《神经漫游者》（*Neuromancer*）迅速风靡全世界。威廉·吉布森承认，创造网络空间一词时受

到了控制论 (cybernetics) 一词的启发。1948 年, 美籍奥地利数学家维纳 (Norbert Wiener) 首先创造了控制论一词, 原意是指船舵 (rudder)、舵手 (steersman)、领航者 (pilot)、管理者 (governor) 等, 所以对于网络空间一词的本身也蕴含着“控制空间”和“控制域”的意思。

威廉·吉布森在《神经漫游者》中对网络空间赋予了一些新的内容, 这本小说把网络空间称为一种“交感幻觉 (consensual hallucination)”, 即电脑爱好者在游戏机前面体验到的直观感觉。威廉·吉布森是一个美国人, 后来移居加拿大, 是一名自由职业者。20 世纪 80 年代初的某一天, 他走在温哥华大街上四处闲逛, 看到一群坐在电子游戏机前面追求精神刺激的年轻人, 他们“一动不动”、全神贯注地盯住电子游戏机屏幕上的图像, 完全沉浸在虚拟的网络世界之中。该网络世界连接了这世界上所有的人、机器和信息资源, 而人在该网络世界的虚拟空间中可以活动或漫游, 思想在那里碰撞并不断创新。威廉·吉布森设想, 如果将这个世界与人脑的神经元直接连在一起, 将会怎样呢? 于是他将电极移植到了小说主人公的头脑中, 变成了人能控制的大脑器官之一, 使其能在这个虚拟的世界中遨游。“从人类系统中每一台电脑的存储数据中, 我们提炼出了一份资料的图解说明。其复杂程度是难以想象的。光路排列在大脑的虚拟空间之中, 即集成的数据中, 就像是肺一样, 不断伸缩。”这个世界是一个巨大的三维数据库, 每一个数据就像街道两旁的灯火一样。威廉·吉布森称这个由计算机所构造的虚拟世界为网络空间。

## 1.2.2 网络空间的基本概念及其架构

网络空间的概念从出现开始, 其含义就在不断发展变化, 解析网络空间相关概念及其关系, 有助于认识联合作战的本质。

### 1. 网络空间的概念与内涵

从结构上看, Cyberspace 由 Cyber 与 space 二者组合而形成, Cyber 表示“计算机”, space 表示“空间”。目前对 Cyberspace 的译法繁多, 有人将它译作“网络空间”, 更有“赛博空间”“异次元空间”“多维信息空间”“电脑空间”“网络电磁空间”等译法。我们认为翻译成“网络空间”更为贴切。这个词的本义是指以计算机技术、现代通信网络技术, 甚至包括虚拟现实技术等信息技术的综合运用为基础, 以知识和信息为内容的新型空间, 这是人类用知识创造的人工世界, 一种用于知识交流的虚拟空间, 是一个具有时域、空域、频域和能域特征的广阔领域。网络空间与陆、海、空、天并列为五大作战空间。

国外学者对“Cyberspace”的定义各不相同。Michael Benedikt 在他主编的 *Cyberspace: First Steps* 中将 Cyberspace 定义为“一个由计算机支持、连接和生成的多维全球网络, 或‘虚拟’实在。在这一实在中, 每台计算机都是一个窗口, 由此所见所闻的对象既非实在的物体, 也不一定是实在物体的形象。在形式上, 其所涉及的符号或操作, 都是由数据和

纯粹的信息构成。这些信息一部分源于与自然和物质世界相关的运作，而更多的则来自维系人类的科学、艺术、商业和文化活动的巨大信息流”。迈克尔·海姆（Michael Heim）在《从界面到网络空间：虚拟实在的形而上学》一书中将 Cyberspace 描述为：“数字信息与人类知觉的结合部，文明的‘基质’，在其中银行交换货币（信用），而信息寻访者则在虚拟空间中存储和再现的数据层中航行……网络空间无所不在，你打电话时，到自动取款机取钱时，都能体会到它的存在。”迈克尔·海姆还将 Cyberspace 描述为：“一种由计算机生成的维度，在这里我们把信息移来移去，我们围绕数据寻找出路。网络空间表示一种再现的或人工的世界，一个由我们的系统产生的信息和我们反馈到系统中的信息所构成的世界。”后来约翰·巴洛在他的“网络空间独立宣言”中将 Cyberspace 描述为一个可以用任何暗示具有空间性的名称来称谓的现实空间，在他看来：“电子通信绝不仅仅是通信高技术，而是已经衍生出一个区间——网络空间，这是一个完全不同的新世界和‘边疆’，它需要一套新的隐喻，呼唤一套新的规则和行为。”

2003年2月，美国政府公布的《保护 Cyberspace 国家战略》中，将 Cyberspace 定义为：“由成千上万互联的计算机、服务器、路由器、转换器、光纤组成，并使美国的关键基础设施能够工作的网络。”

2006年12月，美国参谋长联席会议发布的《Cyberspace 行动国家军事战略》中指出：“Cyberspace 是指利用电子学和电磁频谱，经由网络化系统和相关物理基础设施进行数据存储、处理和交换的域。”

2008年3月，美国空军发布的《美空军 Cyberspace 战略司令部战略构想》中指出：“Cyberspace 是一个物理域，该域通过网络系统和相关的物理性基础设施，使用电子和电磁频谱来存储、修改或交换数据。Cyberspace 主要由电磁频谱、电子系统和网络化基础设施三部分组成。”

在美国2011年《国防部军事及相关术语词典》中，网络空间被定义为：“信息环境中的一个全球范围的域，由信息技术基础设施互相依赖结网而成，包括了因特网、通信网络、计算机系统和嵌入式处理器和控制器”。

维基百科（Wikipedia）中对 Cyberspace 的解释为：网络空间是可以通过电子技术和电磁能量调制来访问与开发利用的电磁域空间，并借助此空间以实现更广泛的通信与控制能力。

综上所述，网络空间是一个通过组网的系统、相关物理基础设施和信息运行环境，是利用电子和电磁频谱来产生、修改、传输、收发、交换、存储、处理、删除和控制信息的空间，是电子战、指挥、控制、通信、监视与侦察的媒介。网络空间以网络结构为主体，以电磁频谱为连接纽带，既包括电磁空间及其扩展和延伸的抽象空间，也包括相关基础设施的物理空间及包括人参与的虚拟环境，是一个从物理设备到信息逻辑，再到人物认知和社会多维活动等众多领域的复合空间，是虚拟与现实的结合体。网络空间集成了大量的实体，包括传感器、武器、装备、信号、连接器、转发器、传输线、处理器、控制器等，不在乎实际的地理位置，以通信与控制为目的，形成一个虚拟集成的世界。在现实中，网络空间构建了相互依赖的信息技术基础设施网络与电信传输网络，如互联网、物联网、无线

电通信网络、信息网络、计算机系统、武器装备平台、综合传感器系统、军事指控网络、金融网、电力网、交通控制网、嵌入式处理器、通用控制器、工业控制系统和人参与的超级时空等。

从字面来看，网络空间就是“可航行的空间”（Navigable Space），即可操纵航向、可进行操作的空間，其实质是泛在的网络电磁空间。

从领域来看，网络空间与陆、海、空、天领域一样，是由电磁波谱、能量传递、电子系统以及网络化信息基础设施组成的一个领域。

从组成上看，网络空间是计算机网络及其所连接和控制的所有事物的统称。

从技术上看，网络空间的作用是使电信、计算机通信和广播电视媒介、感应控制网络等网络融合为一个整合的信息网。

从本质上看，网络空间就是通过对事物的信息化抽取，进一步提高人们的实时控制能力和合理化（Rationalization）管理能力。

从宏观上看，网络空间就是世界的表象空间，其表象的形式是信息。

从微观上看，网络空间就是电子运动的地方，并通过运动实现其所有效能。

从客观上看，网络空间就是一种架构，它使世界以信息的方式被展现。

从表征上看，网络空间是人们与键盘、显示器、鼠标、光缆、工作站、网页等打交道时所面对的一种“敞开”。

从外在表现看，网络空间可分为军事信息网、国家政务网、关键基础设施信息网和国际互联网四类。其中，军事信息网分为作战信息网和军队政务网；作战信息网又可分为战场感知网、指挥决策网、武器控制网、综合保障网、基础设施网等；国家政务网分为保密办公网、政府信息网、专用政务信息网等；关键基础设施信息网分为金融网、电信网、广播电视网、能源控制网、交通控制网以及其他工业控制系统等。

从历史上看，网络空间是人类综合运用物质、能量、信息的空间。

## 2. 网络空间的概念框架

基于网络概念内涵分析，提炼出网络空间的概念框架如图 1-2 所示。

（1）物理实体空间。网络空间是依托物理实体而存在的，物理实体空间描述的是其现实存在基础。物理实体被摧毁，依托其存在的信息系统也随之消亡。

（2）信息运行空间。信息运行空间由语法层和语义层构成。语法层是由逻辑节点组成的逻辑网络结构，逻辑节点依托物理实体存在，是在信息运行空间中可以单独分析的个体，逻辑节点与物理实体是多对一的关系，即一个物理实体可以分解为多个逻辑节点。逻辑网络的边表示节点间存在信息交互行为，这种行为不仅包括己方节点间的通信行为，也包括对抗节点间的信息攻击等行为。语义层包含了信息空间节点拥有的信息以及信息在语法层逻辑网络结构上运行形成的信息流，对信息及信息流的控制是信息运行空间的核心任务。信息运行空间可以概括为基于网络结构的信息运行控制空间，这也是网络空间的本质特性、网络空间作战的核心功能及争夺领域。

（3）社会空间与认知交互空间。社会空间与认知交互空间是两个紧耦合的空间，信息



运行空间中通过争夺制信息权获取的信息优势最终要为社会空间中的自然人进行认知决策服务，社会空间及认知交互空间涉及较为复杂的认知建模问题。

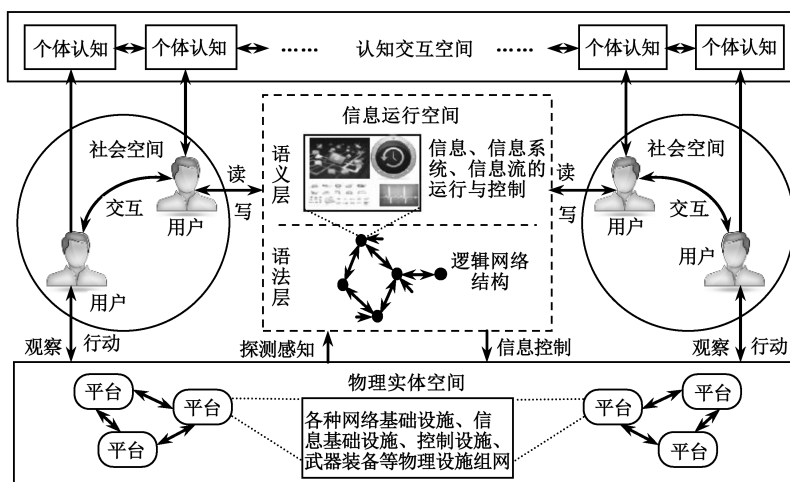


图 1-2 网络空间的概念框架

### 1.2.3 网络空间的组成

网络空间主要由电磁空间“E”和“H”、网络空间“0”和“1”、社会空间“思想”和“人”、物理空间“基础设施”（电子系统和网络系统）组成，网络空间的组成如图 1-3 所示。

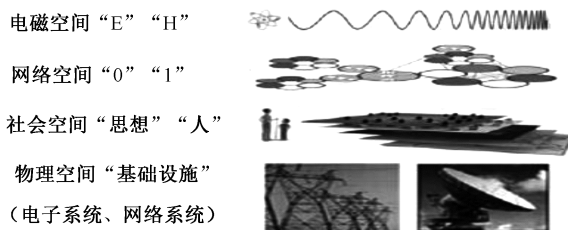


图 1-3 网络空间的组成

网络空间可以从三个层次进行描述：物理层、逻辑层和社会层，如图 1-4 所示。它有 5 个组成部分，即地理组件、物理网络组件、逻辑网络组件、网络角色组件和人员组件。

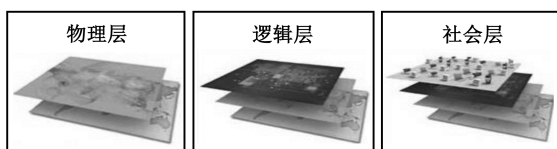


图 1-4 网络空间的三个层

(1) 网络空间的物理层由地理和物理网络组件构成。它是数据传输的介质。地理组件就是网络元件在陆地、空中、海上或太空中的位置。在网络空间中，虽然地缘政治意义上的边界可以很容易地以接近光速的速度进行跨越，但还是存在着与物理领域紧密相关的主权问题。物理网络组件是由硬件、系统软件、支持网络的基础设施（有线、无线、有线链路、电磁频谱链路、卫星和光学设备）和物理连接器（电线、电缆、无线电频率、路由器、交换机、服务器和计算机）构成。然而，物理层使用逻辑结构作为确保安全（例如信息保障）和完整性（例如虚拟专用网络）的主要方法。这是信号情报，包括计算机网络刺探、测量和特征情报、开源情报和人力情报的首要目标。这是第一个用来确定授权的基准点。它也是地理空间情报的首要层次，可以产生有助于网络空间目标选定的有用数据。

(2) 逻辑层包括逻辑网络组件，其本质是技术性的，主要指网络节点间的逻辑连接。网络节点可以是连接到网络的任何装置，如计算机、电台、个人掌上电脑、手机等。它是从物理网络抽象出来的表示一个网络与另一个网络关系的那些元素。

(3) 社会层由人及认知要素组成，包括网络角色组件和人员组件。网络角色组件包括网络上人员的身份和角色，如 E-mail 地址、计算机 IP 地址、手机号码等。人员组件则由网络上的实际人员组成。一个人可能担负多个网络角色，比如一个人可以拥有多个电子邮件账户，而一个网络角色也可能被多个人员使用。社会层表示对网络空间中的逻辑网络的一个更高水平的抽象；它使用了适用于逻辑层的规则，开发出一个表示网络空间中的个人或实体之身份的数字表示。

#### 1.2.4 网络空间的特点

网络空间呈现出许多新的特点，下面将进行详细介绍。

##### 1. 互联无边界性

由于各国的计算机网络系统都是互联的，凡是网络所覆盖的区域都是其作战范围，在当前网络空间中，网络线路的数量正在呈指数级增长，作战环境中所涉及的因素较多，随着网络技术的发展，将有越来越多的要素加入网络中，网络互连程度日益加深，在不久的将来我们有望看到无处不在的相互连接的电子设备和终端。

由于电磁频谱缺乏地理界限和自然界限的限制，这使得网络空间触角几乎可以伸向世界的任何一个地方，可以超越通常人为所规定的组织和地理界限，没有前线和后方的区分，可以跨越陆、海、空、天全领域进行人类活动，成为日益增大的公共域。网络空间几乎可覆盖任何区域，凡是电磁波能到达的地方都是网络空间的范围。

网络空间广泛分布、开放参与，不存在中心控制；有着无数的聚合与分离、在线与离线、创建与删除等情况发生。很难在世界上找到一个不受网络空间影响的地方。信息可以连续、无缝地穿越政治、宗教、文化和地缘的界限，甚至网络空间的基础设施（软件和硬

件)的设计、生产和发展已经全球化。每种新的计算机服务器或互联网手机的出现,每一颗卫星的升空或增加一个地球站等都会扩展它的边界;每一次信息化战争的出现都会大大扩展它的空间,在实时对抗中此消彼长。网络攻击武器可以从世界任何地点攻击其他任一地点,没有了爆炸硝烟,模糊了平时战时,缺失了国家边界,超越了地理疆界。

网络空间与传统空间相比,使得地理空间的作用相对减弱;在数字化世界里,距离的意义越来越小,注重的是网络上的到达。在力量的组成上更加注重逻辑上的联合,使远程观测、实时跟踪、遥距控制等成为可能,并以前所未有的方式和速度突破地缘在时间和空间上的阻碍。全世界因各种信息系统而连接在一起,使得“一网打尽全世界”成为可能。

## 2. 几何度量性

网络空间是通过电磁频谱及能量来实现的,是提供信息不间断流动的空间或媒介。网络空间虽然不存在传统意义上的高度、深度和长度,不能单以客观统一的尺度去测量,但却具有几何性质。虽然电磁频谱看不见,但是具有可以测量的物理范围,可以用能量、波长或频率等术语来表述;有独特且唯一的度量标准,通过独特的度量,网络空间可以呈现各种不同形式,如计算机游戏、超媒体、虚拟现实、脑机界面、战场统一态势感知显示等,可以用来绘制其边界和操作地图。

采用某些技术绘制网络空间地图,可清晰地表明网络空间的通信线路和关键节点具有战术和战略意义,以便能对其进行更好的控制。这些关键节点有的可能是物理节点,有的可能是信息节点。

## 3. 分散异构性

网络空间是由很多不连续的网络节点和链路构成的,因而是一个不连续的、极度分散、动态且持续演变的域。单个的网络空间节点可以存在于陆地、空间卫星、飞机以及舰艇。网络空间的互联程度日益紧密,但其网络可以通过多种方式进行隔离。协议、防火墙、加密以及物理隔离等是把某些网络与其他网络(例如互联网)相互隔离的基本手段,阻止网络空间数据被窃取和攻击的有效办法是与任何网络物理隔绝,禁止能量与外界的交流。也可通过建立网络来有效隔离大多数射频入侵。网络空间是一个异构的域,由很多小型的、分散的分系统等组成其整体结构。网络空间由很多功能、互联程度、技术复杂性以及脆弱性各不相同的不同类型的网络组成,通过协议、接口以及基础设施的标准化可实现不同分系统之间近乎无缝的信息交换。

## 4. 变化创新性

网络空间的部分改变是来源于技术创新,包括组件和网络协议的添加、移除、更换或重新配置。网络空间随着信息和通信技术的发展而不断变化。同时,网络空间作为一个区别于传统空间的新领域,对其内涵的理解也在不断地深化之中,并引发人类对新的空间领域、国防安全与战略、新的作战与行动等认识和理念发生重大变化。技术的创新及高速发展为网络空间提供了巨大的创造力和可能性;谁拥有更新的技术,谁将在网络空间中占有

更多的优势，就会拥有网络空间的领导地位。与此同时，要求作战人员具备相当的专业知识，与技术革新发展保持同步。

## 5. 低值高能性

进入网络空间和进行常规访问的成本极低，接入限制极少。对于优势技术和行动资源的需求是非常低的，进入障碍、风险和技术门槛都是非常低的，几乎一台笔记本电脑的成本，或简单地通过鼠标与键盘就可以轻松地访问、使用网络空间，只需敲几下键盘就可能引发大规模网络战甚至热战。网络武器的研发不需受材料以及被严密保护的信息限制，技术普通，成本低廉。网络武器使用简单快速，障碍不多，无须授权，也无法正确评估它可能带来的一系列后果。网络空间作战能够凭借较低的成本获得极高的军事价值。同时，通过网络空间，可以用较低成本，迅速对兵力进行部署及远程控制，广泛地获得各种战斗能力和作战行动。

## 6. 实时高速性

发生在网络空间中的作战行动表现出前所未有的速度，这种速度被称为“网络速度”。网络空间的态势常常以虚拟现实短暂存在，动态与重构往往瞬间进行。在网络空间中，信息以比特流的形式进行传输，这种比特流在有线和无线介质中以电信号或光信号的形式传输，其速度使得它能够让信息在瞬间遍及网络所能联通的任何角落，延迟几乎忽略不计，传统的时空限制已经被打破。网络空间中的行动速度以光速爆发、展开或推进，为通过遥远的距离并以极快的速度施加各式各样的实际影响提供了可能性，如果不采取快速行动将丧失作战良机；被攻击的网络即使在数秒时间内也容易发生连锁反应，也更容易跨越国界。因此，在一定的情况下，网络空间能够提供快速决策、指挥、控制、反击和实现预期效果的反应能力，但也导致了危机的不稳定性，让战争处于千钧一发状态，没有思考时间。

## 7. 虚拟隐蔽性

网络空间不像陆、海、空、天空间一样自然存在，它是信息技术和社会信息化程度发展到一定阶段的产物，是一个物质与虚拟相结合的共同体，有形与无形相统一的客观存在的新质作战空间。网络空间是思维自由驰骋、自由想象和自由构绘的空间，是现实空间的映射，是自然空间的逻辑呈现。

网络空间的隐蔽性表现在没有有效的能够对网络空间中发生的攻击行为进行提前预警的工具，在己方没有受到攻击之前，己方并不能知道己方网络之外的哪几个点将会对己方的哪个目标发动什么攻击，攻击方会试图隐藏自己的身份和使用的路由器，当己方受到攻击后也可能并不知道攻击源的真正位置。一方面，可能绝密数据从某网络中被泄露且无能为力，而事件很久后才被察觉发现；另一方面，匿名性及归属问题始终存在，攻击者可以采用未经授权的协议或虚假信息进行身份隐匿，有的故意隐藏攻击行为并消除其痕迹；这就对想要隐藏在网络领域的使用者进行侦查、追踪和锁定提出了很大的挑战；确认犯罪等行为及其动机非常困难，攻击实力被隐藏，攻击者难以确定，甚至被误导。

## 8. 易损脆弱性

由于物理空间有电磁辐射,由于互联网有漏洞,由于电子系统软硬件有漏洞,由于信息系统配置有缺陷,由于越来越多的关键系统连上互联网,因而网络空间安全问题也越来越突出,存在很大的易损性、脆弱性。对于空间无线链路,不仅开放性大,而且卫星平台上的链路设备受到体积、重量和功耗的严格限制,抗截获、抗干扰等手段往往十分有限,脆弱性尤为突出。对于空间网络和卫星上的计算机来说,由于空间数据传输延迟大,数据误码率高的特点,加之空间环境条件恶劣,空间应用的硬件、软件有特殊要求等因素,空间网络抗攻击能力难以提高。因此,通常网络空间是脆弱的。

## 9. 关联社会性

所有的空间——几何空间、物理空间、社会空间、想象空间、文本空间等都可以向网络空间“投影”,更重要的是网络空间嵌入到人类真实的社会文化系统之中,带来了人类社会关系和生活方式的变革。对大多数人来说,网络空间是不定型、不透明的,网络空间似乎成为一个新的公民社会。网络世界由信息传输、关系互动和思想本身组成,复制、虚拟和出位揭示了主体在网络空间中共存与在现实空间中共存的差异,呈现新的可能性,统一性和普遍性正被特殊性和多样性所取代。传统法律制度下的公共权力无法解决网络空间带来的特殊问题,例如管辖权问题、公共权力的法律后果难以确定等。信息和知识的加速商品化,使网络空间成为一个整体市场,信息、知识和网络都成为经济学意义上的隐喻,网络空间最终可能会演变为虚拟资本主义的新边疆。

在网络空间中,一个人员可以同时充当多个角色,例如一个网络战士(黑客)可以同时使用多个攻击软件。一个角色可以对应多个人员,例如一种软件可以供多个人使用。

## 10. 全天候一体性

网络空间几乎不受外界自然条件的影响,没有气候因素、地理环境以及白昼和黑夜的干扰。从一定意义上讲,它可以进行全天候连续作战。

网络空间是一个跨越国家和行业,把整个世界连为一体的空间;它把分散于陆、海、空、天的空间所相互依赖的信息技术基础设施网络视为一个整体;把传统的、相对独立的人造信息系统和电磁环境作为一个内在联系的有机整体。网络空间各要素一体化交互运用、协同行动,支持各类传感器的集成、态势感知的数据集成、全球作战集成和统一的攻防行动集成。它具有作战力量多元一体、战场空间多维一体、信息系统多类一体、对抗行动多样一体的独有特征。

## 11. 开放包容性

电磁空间和信息网络空间是开放的,任何人都可进入网络空间,成为网络人员。网络空间的有线和无线传输链路、接口、传感器和节点开放性大,有时甚至连它们的参数都是公开的。从另外一个角度来说网络空间具有极大的包容性,包容着信息、航空、航天、海

洋、电力、交通、医疗、能源、教育等多个行业。从宏观到微观，从实体到虚拟，从物质到认知，涉及人们生活的方方面面。

## 1.3 网络空间作战的内容特征和能力要求

### 1.3.1 网络空间作战的概念和相关问题

#### 1. 网络空间作战概念

网络空间作战是指围绕争夺网络空间控制权而展开的各种技术战术行动。网络空间的控制是有效实施战略、战役、战术等各层次作战行动的基础。通过控制各种网络和电磁频谱，综合利用一体化的监视、侦察、态势感知和战场管理等能力，将信息渗透到陆、海、空、天实体空间，把所有作战领域内的活动和装备连接起来形成作战系统，实现相互协调配合的作战行动；同时，利用网络空间武器来压制和摧毁敌方在陆、海、空、天等领域的基础设施和电子攻击系统，达成作战的态势优势。

网络空间作战的本质是通过更新和发展相关技术，利用、控制、建立信息和信号所引发的攻击或防御信息系统，提高网络空间的信息负载能力、能量传输水平以及对信息的处理和控能力，为指挥官提供关于执行决策、促进作战以及把握作战机遇等方面的增强性手段，在各种侦察与反侦察对抗上获得信息优势，在作战行动中削弱或消除敌方的军事能力，并最终赢得战争。

网络空间作战是在网络空间内或通过网络空间，开展的军事活动、情报活动和日常业务运营，运用网电能力而达成军事目的或军事效果的作战，既包含了网络化的电子战，也包含了现代的网络战及其心理战等。

电子战，对电子目标实施干扰，进行反辐射攻击，利用电磁能摧毁敌方电子系统。

网络战，是以计算机、计算机网络和互联网为依托，围绕“制信息权”的争夺，以先进的信息技术为基本手段，以有线网络和无线网络为战场，以武器控制、指挥、控制、通信、计算机、情报、监视与侦察（C<sup>4</sup>ISR，Command、Control、Communication、Computer、Intelligence、Surveillance、Reconnaissance）等系统中的核心设备——计算机为主攻点，利用敌方网络信息系统自身存在的安全漏洞和其电子设备的易损性，通过使用网络命令和专用软件进入敌方网络系统或使用强电磁脉冲类武器摧毁其硬件设施的攻击，从而达到篡改、伪造数据，干扰、中断、破坏敌方计算机、网络设备和计算机控制系统，并保证己方网络化信息系统的正常运行的目的，进而夺取“制信息权”。最主要的手段：一是释放计算机病毒，二是网络“黑客”攻击。网络战可在瞬间发生，没有固定场所，从银行到国家

防控体系，人们依赖的系统都有可能成为攻击目标，其后果是真实的且能快速波及全球。

心理战，通过网络空间的虚拟作战演习，在心理上给对手造成震慑，利用网络空间信息传播的全球性，了解军事人员、技术人员乃至普通百姓的思想动态；这种手段不仅用在战时，也可以在平时应用。战场上军事斗争的双方实际上是在对这种信息控制权利的保持与争夺。由于其作战媒介包括存储或传输、物理或虚拟、静态或动态、电子或光子等多种形式，所以网络空间作战又不同于传统的信息化战争。

网络空间作战是集物理、逻辑和认知攻防于一体的作战，网络空间作战概念示意如图 1-5 所示。

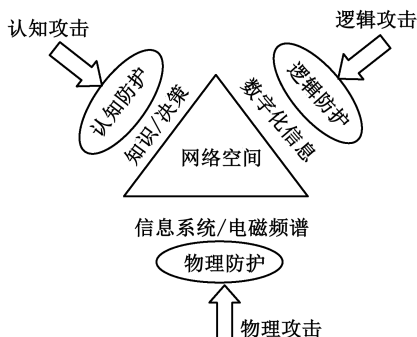


图 1-5 网络空间作战概念示意

在物理层，物理攻击主要是运用各类动能和非动能武器，对网络空间的物理载体进行攻击，破坏、限制敌方的情报系统、指挥网络和武器打击系统，甚至使之瘫痪。物理攻击还包括对敌方信息系统和相应基础设施，以及决策人员的直接物理攻击等。在物理防护方面，主要是增强对电子系统的物理防护，避免被敌方武器杀伤。

在逻辑层，逻辑攻击通过向敌方网络发动计算机病毒攻击、逻辑炸弹攻击等方式实施网络阻塞攻击，或利用无线信道向敌方网络植入病毒，干扰、破坏敌方计算机与计算机网络系统，造成敌方指挥控制系统瘫痪。在逻辑防护方面，主要通过网络的冗余性、增强自动入侵检测能力、采用恶意程序保护等手段进行抵御。

在认知层，认知攻击通过制造一些虚拟信息欺骗，误导对方操作，对敌方的决策与指挥控制产生信息误导和流程误导，造成其决策和指挥失误，或者通过直接渗入敌方各类信息系统，获取敌方网络电磁空间的控制权，接管并控制敌方各类电子信息系统，给敌方造成毁灭性打击。在认知防护方面，主要通过反情报、真假信息识别，以及增强系统鲁棒性等方法提高反欺骗、反渗入和反控制能力。

## 2. 网络空间作战的主要样式

网络空间作战主要以计算机和通信网络以及设备、系统和基础设施的嵌入式处理器与控制器为目标，利用网络空间态势感知、网络空间作战攻击、网络空间作战防御和网络空间作战支援来相互支持。它主要涉及构建、运作、管理、保护、防护以及指挥和控制作战网、重要基础设施关键资源，以及其他具体的网络空间。

目前，网络空间作战主要包括网络空间态势感知、网络空间作战攻击、网络空间作战

防御、网络空间作战支援四种作战样式。

(1) 网络空间态势感知，是在网络空间条件下，对环境内要素的感知、要素意图的理解以及要素近期和未来状况的预测，理解任务对具体资源的依赖、资源之间的相互依赖关系和任务之间的相互依赖关系，通过评估与分析来理解态势意图，将信号转换为警报，为蓝色、灰色和红色系统实时收集并长期维护有意义的数据，以满足网络空间内各领域的作战需求。

(2) 网络空间的作战攻击，就是拒止、降级、削弱、中断、操纵、摧毁或欺骗敌人，确保在网络空间内己方自由行动的同时，拒止敌方自如地采取行动。主要行动包括实施电子系统攻击、电磁系统封锁与攻击、电磁干扰攻击或欺骗、网络攻击和基础设施攻击等。诸如施放病毒、窃取篡改数据、服务拒绝、引爆网络炸弹等，在瞬间完成瘫痪、破坏敌方的信息网络。攻击目标包括敌方的地基、空基和天基网络等。由于敌人对网络空间的依赖性越来越强，因此网络空间进攻性作战可实现的潜在作战效能将越来越大。其效能主要包括传感器破坏、数据控制、决策支持降级、指挥控制破坏、武器系统降级。网络空间进攻的手段隐蔽性强，攻击行动速度快，时间短，敌方还没有来得及发现，攻击行动就已经完成，具有很大的欺骗性和隐蔽性，难以一一检测和监视。

(3) 网络空间作战防御，包括在敌方攻击前、攻击过程中，以及攻击后所采取的旨在保存、保护、恢复以及重建己方与友方网络空间能力的措施与行动，对攻击己方信息网络的未经授权的活动或警报/威胁信息做出响应，并根据要求利用情报、反情报、执法和其他军事能力开展活动。比如：网络空间攻击威慑、网络空间攻击缓解与抗毁能力；攻击源跟踪、脆弱性检测与响应、数据与电子系统防护，以及电磁和基础设施防护；等等。

网络空间作战防御包括战胜对手，或应对内部和外部的网络空间威胁，响应攻击、刺探、入侵网络上的恶意软件的效应。大多数网络空间作战防御发生在采取了防御措施的网络内。内部防御措施包括任务保障措施，以动态地重建、维护、重排、重新路由，或隔离降级的或被攻破的本地网络（驻地网络），以确保联合部队、指挥官部队有足够的网络空间访问能力。网络空间作战防御使命是通过分层的、自适应的、深度防御的方法来完成，而且数字和物理保护相互支持，采用主动网络空间防御的措施协同地、实时性地发现、侦测、分析和减少威胁和漏洞，以保护网络和系统。网络空间作战防御和响应行动必须根据常规交战规则和任何可以适用的补充交战规则授权，在某些情况下，采用反制措施。

网络空间作战防御包括电磁空间作战、网络作战方面的防御。电磁空间作战防御主要是空间链路电子防护、电磁抗截获、抗干扰措施，包括时域、频域、空域、极化域、信号域等抗干扰措施。网络作战防御主要是信息安全、网络防护等措施。包括身份验证、多重加密、数字签名、病毒查杀、入侵检测、网络盾牌等措施。

纵观各国网络空间的作战能力建设，建立安全评估、监控预警、入侵防御、应急恢复相结合的防御体系，把主动防御和纵深防御相结合，防止秘密信息被泄露到互联网上；特别是防止黑客和他国情报机构对己方网站进行攻击，被视为赢得网络空间作战主动权的重要前提。

(4) 网络空间作战支援，是为了专门保障网络空间作战和网络战争而形成和应用的各



种支援活动的集合。网络空间作战支援包括漏洞评估、基于威胁的安全评估、漏洞/安全补救、恶意软件逆向工程、利用网络电磁能力使节点为己所用、反间谍活动、网络电磁刑侦术、执法、网络空间研究开发以及试验和鉴定、网络空间作战发展与采办。

### 3. 网络空间作战的基本范围

网络空间作战主要在以下四个层面展开：

一是信息基础设施，也就是计算机和通信设施的联网，包括有线、无线通信设施、通信卫星、计算机等硬件设备；

二是基础软件系统，包括操作系统、网络协议、域名解析等；

三是应用软件系统，包括金融、电力、交通、行政、军事等方面的软件系统；

四是信息本身，针对在网络中流动的所有信息。

严格地说，对信息基础设施的打击应归为广义上的网络空间作战，它针对的是网络运行的基础。虽然各个国家和地区在定义网络空间作战概念时，并没有将信息基础设施完全纳入网络空间作战的范畴，但是，现代战争一旦打响，对信息基础设施的打击却是第一位的。

### 4. 网络空间作战的组成要素

为在网络空间获取战略优势，下列要素至关重要：

(1) 进攻/防御作战。进攻作战与防御作战必须能够相互支持，军队才能真正拥有最强的网络空间作战能力。

(2) 通力协作。想要在网络空间实施作战并实现预期作战效果，组织机构、作战能力、系统功能、技术支持等诸多方面的通力协作是必需的。

(3) 信息共享。必须能够在网络空间内共享信息，进而支持作战。与此同时，需要有配套政策和技术体制来支持有效、安全的信息共享。

(4) 指挥关系。作战指挥关系的顺畅、响应度、直接性、灵活性和机动性直接影响网络空间军事力量的有效运用。

(5) 指挥与控制。网络空间为陆、海、空、天域军事行动的指挥控制奠定基础，由于网络空间的固有特性，网络空间作战的指挥控制要求决策周期更短。

(6) 配置管理。必须能够对支持网络空间作战的各系统实施有效控制。实施配置管理能够实现对网络空间工具、程序、进程等的应用，这对于一个成熟且具备抗攻击性的网络空间来说至关重要。

(7) 执行力度。管理机构要不遗余力地推动网络空间政策的执行力度，同时根据新技术突飞猛进带来的新问题、新情况对政策进行修订补充。

(8) 对网络空间的认知。军队各级还将进一步加强对网络空间的认识和了解，将其与传统的军事作战、情报作战和业务运行一并考虑。

## 5. 网络空间作战的基本需求

网络空间作战基本需求包括：

- (1) 快速应对网络空间的攻击和重新组建网络，保护重要国家基础设施；
- (2) 全域空间内集成网络战力量，获取全球和战区的网络空间运行效果；
- (3) 通过网络空间战胜敌方新样式的作战；
- (4) 支持己方指挥员在网络空间中的行动自由；
- (5) 连续的网络空间态势感知。

### 1.3.2 网络空间作战的本质特征

任何空间的战略博弈，本质上都是国家和利益集团对空间主导权、控制权的追求，并以此维护权益，拓展利益。同时，不同空间战略博弈在本质属性上存在着差别，由此决定了不同空间争夺的不同特征。

#### 1. 网络空间作战的本质

回顾各类空间的作战博弈，核心都是谁占主动、谁说了算的问题，网络空间作战也不例外。网络虚拟空间与传统实体空间的区别在于，传统空间是自然界的产物，作战博弈是国家矛盾在现实世界里的自然延伸，博弈结果通常为占据某一空间地域、形成力量优势；网络空间则是科技界的产物，战略博弈是各种矛盾在现实和数字世界里的集中映射，博弈结果通常为渗入多个空间领域、形成控制优势。换言之，前者作战博弈通常围绕一域进行，而后者作战博弈将贯通全域展开，并呈现出从虚拟到实体、从微观到宏观、从软件到硬件、从精神到物质的综合性抗衡态势。

可以说，要不要在网络空间展开作战博弈，不以人的意志为转移，而受空间斗争规律制约，是人类发展阶段性矛盾的必然结果。要维护网络空间安全秩序，就必须直面网络空间作战博弈的现实，提高博弈能力，将正能量做大做强，并具体落实到不断加强“硬实力”和“软实力”上。网络空间作战博弈“硬实力”，将主要由技术先进、产业领先、自主可控、攻防兼备等方面的内容构成，是综合国力在网络空间的具体体现；网络空间作战博弈“软实力”，将主要由网络发展战略清晰、网络文化繁荣发达、网络管理健康有序、网络教育人才辈出等方面内容构成，是综合素质在网络空间的具体体现。可以这样比喻，“硬实力”是“软实力”的千斤顶，“软实力”是“硬实力”的倍增器。软硬两手不可偏废，不可分离，只有两手都有，两手都硬，网络空间作战博弈才有资本，才有底气。

#### 2. 网络空间作战的特征

与传统的作战模式相比，网络空间作战的特征主要表现在以下几个方面：

(1) 作战战略的威慑性。传统领域内的战略威慑,主要通过载有核武器的各种平台实现的;而网络空间内要想实现战略威慑,则通过使得敌方高层领导觉得自己国家的战略基础设施,始终处于对手网电攻击的阴影之下,而不敢轻举妄动。网络空间的战略威慑作用还表现在平时通过虚拟演兵展示其网络空间作战能力,并产生对对手的心里的一种作用和影响,包括战场性虚拟对抗演兵及对政治、经济、人文的影响演兵;也表现在战时对战争潜力目标、人文心理施加的作战影响。

(2) 博弈技术上的先进性。网络空间作战,比的是智慧,拼的是科技,是网络基础设施核心技术、网络系统应用服务技术、网络攻防作战实用技术的发展竞赛,呈现出高新技术广域融合的趋势。网络空间对抗的手段具有高智能性和知识性,分析和发现各种硬件、操作系统和应用软件的漏洞,并研发出有效的利用工具和攻击武器来抢占网络战的制高点,是一项技术性非常强的工作。网络武器需要利用丰富的电子技术知识和高新技术,对作战人员的知识要求较高。在网络空间作战中,胜负绝大部分取决于网络技术能力。如果疏忽网络防御,传统军事大国不见得稳居上风;若攻击其网络的关键点,武力弱者亦可扭转劣势,反败为胜。

(3) 作战武器工具的局限性。网络空间作战目标的攻击具有明确的针对性,每一种作战武器只能针对具有一种或某一类系统弱点的作战对象来实施。随着网络软硬件系统版本更新升级,原来的武器就会失效,必须研究和发现新的系统或设备的弱点,并研制新的攻击武器。

(4) 作战指挥管理的复杂性。网络系统由于技术的不断发展,变得更为复杂,网络空间作战的指挥管理也随着网络系统的动态变化而变化。有时隐蔽无形、藏头掩尾,有时公开亮剑、推波助澜,呈现出变幻多样的复杂形态。有时战争来无影去无踪,没有硝烟,没有设施损毁或人员伤亡,但却影响甚至决定了战争走势和胜负的作战效能。

(5) 作战手段的多元性。与传统意义上的作战相比,网络空间作战力量及手段更加多元,其运用更加灵活,已不单单是传统的电子对抗、网络对抗作战单元的对抗,还包括新型网络作战单元及其之间的对抗,更包括综合利用陆、海、空、天这四维战场空间中通过网络互联的各种网络作战单元及作战手段的对抗,涉及信息感知与控制相关的所有领域,包括各类 C<sup>4</sup>ISR 系统和指挥控制活动,同时也包括对国家战争潜力系统、国家关键基础设施控制网络等所采取的网络行动。

(6) 作战体系的对抗性。网络空间作战远远超过了战场作战范畴,涉及政治、经济、外交、军事和社会等战争全领域,是战争层面的体系对抗。在战场对抗领域,网络空间网络是作战体系的基础,又是网络空间作战目标,在这种复杂网络战场下的作战是一种典型的体系对抗作战。在战略网络空间内作战,不单单因针对战争潜力目标网络就说是体系对抗,更重要的是对战争潜力目标网络实施网络行动后所产生的级联效应。

(7) 作战组织的综合性。随着网络空间日益膨胀和对国家安全与利益的影响越来越大,网络空间作战正从最初散乱无序的“黑客”行为、企业行为、军事领域专项行动等,发展为“国家主导、军队主体、各方参与”的国家组织行为。随着网络空间战略博弈越来越跨界展开,促进了国家间网络空间联盟、联防和联合演练的实现,尤其是虚拟空间的军事联

盟更是迅速发展。网络空间战略博弈较量正成为国家间斗争的全新形式。

(8) 作战系统的控制性。控制各种信息系统和体系的运作是网络空间作战取胜的重要标志。网络空间对各种作战行动和决策的影响,主要体现在为决策人员提供可信和可用的信息,并能将决策信息安全可靠地下发、传达,而这些能力只有在各种信息系统和体系被有效控制和安全运作的情况下,才能实现。

(9) 作战力量的广泛性。信息技术的军民通用性和计算机网络的互联开放性,使得网络空间作战的力量非常广泛,社会上的任何组织和个人都有可能成为军队网络空间的作战伙伴,战争将不再是军人独占的舞台,而是国家甚至非政府组织乃至个人都能实施的普通行动。

(10) 作战行动的隐蔽突然性。在网络战场空间中,没有人体器官可能感受到的“特质流”和“能量流”,只有静静流淌的“比特流”。“比特流”虽然可以用电子仪器显示出来,但对于网络攻击,甚至在攻击造成了破坏效果后,我们有可能不知道攻击来自何方,作战对手是谁,战争可以在公开敌对的时期进行,也可以每天进行隐蔽战斗。

(11) 作战投入的高效性。开发网络空间作战的攻击技术,不像研制和生产杀伤性武器那样需要巨大的人力、物力和财力支持,只需要具备信息系统专业技能和少量资金就能进行。同时,无论是任何组织和个人,只要具备相应的计算机知识,掌握一定的网络攻击手段,都有可能变成可怕的网络杀手。

(12) 作战时间空间的超常性。网络空间作战在时间空间上已经远远超出了常规范畴。在时间上,具有瞬间实施机动和渗透的作战能力,可瞬间转移网络空间作战力量,任何时间发生交战,攻击力都可以光速到达攻击目标,瞬间完成网络空间作战任务。另外,也可以是持久作战。在空间上,网络空间作战是“大范围”“多领域”,可施效于全球范围、传统作战空间和网络空间,无明显的“前后方”之分,具有“跨域”作战和无界作战特性。通过网络战、心理战、舆论战、情报战和正常网络交互活动等方式不间断地扩展开来,斗争越来越呈现出常态化、白热化的状态。

### 1.3.3 网络空间作战的内容形式

网络空间作战的内容和相应的形式可分为网络情报活动、网络作战指挥、网络攻防对抗、网络实体控制、网络舆情导控、网络价值博弈、网络规则制定、网络技术比拼、网络服务保障九个方面。这些内容形式包括相关的能力和活动,相互结合,以帮助联合部队指挥官集成、协同、指挥联合作战。下面介绍每个内容形式如何适用于利用网络空间进行的有效联合作战行动。

#### 1. 网络情报活动

据美国情报机构统计,在其获得的情报中,有 80%左右来源于公开信息,而其中又有

近一半来自互联网。

网络情报活动是网络空间作战和安全斗争最活跃的部分，主要指围绕承载高价值情报的军事网络、民用网络、用户终端等，展开窃密与反窃密斗争。网络情报活动较量无声无形，“网络战士”使用病毒、木马、黑客软件等手段，足不出户就能获取极有价值的各类情报，这是隐藏在计算机屏幕后面的战斗。由于互联网上获取军事情报信息量大、机密等级高、时效性快、成本低等原因，依托互联网开展的情报侦察活动已经无孔不入，而且防不胜防。当你浏览网页或与朋友网上聊天时，可能不知不觉就被“对方”牢牢“锁定”，成了“网谍”的猎取目标。

从现实效果看，情报活动一经与网络结合，便产生惊人效益，凸显出深渗透、低成本、高效率等特点。其活动，一方面是围绕各类网络传输信息的截获与反截获展开，包括组织信道接入、密码破译，以及信道加密、信息加密等；另一方面是围绕各类网络终端的信息窃取与反窃取展开，包括组织入侵检测、漏洞修补，以及破译密码、控制主机、隐蔽潜伏、回传信息、消除痕迹等。具体的情报活动和过程如下。

(1) 在网络空间收集到的情报可能来自军队或国家一级，可能服务于战略、战役或战术要求。网络空间的军事情报面临独特挑战，需要掌握军事情报联合作战条令的基础知识。

(2) 了解作战环境是所有的联合作战行动的基础。网络空间作战的情报支持采用所有其他军事行动中的相同的情报过程和行动。

① 规划和决定，包括管理情报界的活动，以防范针对用户/设施的间谍、破坏和攻击活动；审查任务成功的标准和指标，以评估网络作战的影响，并告知指挥官，做出决策。

② 收集，包括监视和侦察。

③ 处理与利用收集到的数据。

④ 信息分析，形成情报产品。

⑤ 分发和整合可靠情报。

⑥ 评价和反馈有关情报的有效性和质量。

(3) 事件侦测和表征。一个变化莫测、技艺高超的对手在网络空间实施的活动一般难以察觉。不像物理域的敌对行动，可以通过检测设备或特定活动而发现，在网络空间中的敌对活动可能不容易与合法行为区分开来。侦测和追查网络空间活动的的能力，对于实现有效的防御性网络空间作战和进攻性网络空间作战是非常关键的。同样重要的是，快速评估军队利用网络空间进行的行动，有助于快速改变战术、防御措施以及其他可用响应方案。

(4) 为了尽量减少利用先前未知安全漏洞的威胁之影响，联合部队应该制定缓建和恢复措施，包括演习在网络空间的部分被拒阻或攻破情况下进行操作的能力。

(5) 分析和追查。因为网络空间作战中的物理网络、逻辑网络、网络行为体的特征，在追查敌对的进攻性网络空间作战中，找到具体的人、犯罪组织、非国家行为体，甚至是负责任的民族或国家，是很难的。

(6) 情报收益/损失。另一个值得关注的是，网络空间作战可能危及情报收集活动。在执行网络空间作战之前，在最大可行程度上进行情报收益/损失评估是必需的。情报收益/损失评估被大量的在网络空间运作的不属于军方的政府部门以及跨国合作伙伴进一步复

杂化了。

(7) 征候和警报。对造成国家威胁的网络空间情报的分析，应包括所有来源的情报，这样才可能寻找到传统的政治/军事征候和警报。敌对的网络空间行动往往会出现常规敌对军事活动外，并经常提前发生。此外，网络空间征候和警报可以识别对手网络空间作战触发标识，但仅只有相对较短的时间来做出响应。因此，有必要把所有来源的情报都加以分析，以至于能够有效分析敌人在网络空间的意图。

可以将网络空间情报分为三类：物理层情报、逻辑层情报和社会层情报，其中每一类均应包含己方、敌方和其他网络空间的情报。网络空间的情报分类如图 1-6 所示。

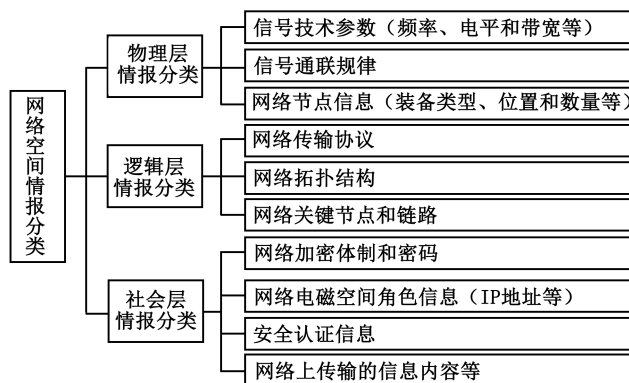


图 1-6 网络空间的情报分类

其中逻辑层和社会层的情报侦察活动均属于网络行动的范畴，而物理层情报保障则必须由电子战情报实施保障，属于电子战的范畴。对上述物理层情报实施电子侦察时，主要利用电子情报侦察装备，对敌网络空间有意或无意辐射的电磁信号进行搜索、截获、定位和识别，从而获得敌网络空间的无线电信号特征和技术参数，通联规律，网络节点的装备类型、数量、部署、位置 and 变化等信息。其中有意辐射的电磁信号主要是网络通信信号；无意辐射的电磁信号主要是指电子设备无意泄漏的信号。据试验，使用专门的电子侦察设备，可以在几十米甚至几百米外，截获计算机辐射的电磁信号。通过对逻辑层、社会层目标的情报侦察，可以进一步分析出敌方网络空间的漏洞、评估敌方的网络电磁能力和意图等；而通过对物理层情报的电子侦察，则可以找到敌网络空间的无线接口及链路，把握其网络通联规律，对其网络空间节点进行精确定位，为己方进入敌网络空间提供了可能，也可为下一步的电子战行动提供情报信息。因此，电子战情报保障是网络空间作战情报保障不可或缺的一部分，网络空间作战的顺利实施，电子战情报保障将发挥着不可替代的作用。

## 2. 网络作战指挥

利用网络空间作战的指挥包括指挥官行使职权，对下属部队下达命令，并促使任务的完成。联合部队指挥官提供作战愿景、指南和方针给联合部队。就他们的角色而言，提供通信通道、规划和决策支持辅助和相关的网络情报、监视和侦察（ISR，Intelligence、

Surveillance、Reconnaissance), 网络空间作战可及时获取关键信息, 可以使联合部队指挥官比对手更快地决策、执行决策, 使指挥官能够更好地控制作战时机和节奏。

(1) 网络空间作战需要统筹行动, 团结力量, 来实现一个共同的目标。然而, 网络空间作战的双重性质——同时在全球范围内以及在战区或联合作战区域层次提供行动——就必须适应传统的指挥与控制结构。联合部队主要采用集中作战规划与分散作战执行的模式。某些网络空间作战功能, 特别是全球防御, 需要集中执行, 以满足行动的多种的、瞬时的要求。然而, 这些网络空间作战必须与联合部队指挥官的区域或本地网络空间作战整合和协同, 由分配给或附属于联合部队指挥官的部队执行。

(2) 不同的指挥结构可以为联合部队指挥官提供一个独特的部队组织和编组。进行网络空间作战活动的部队的指挥是由联合部队指挥官执行的。

① 军队信息网络运维需要集中协调, 因为它们可能影响军队信息网络的完整性和战备。虽然执行一般会分散化, 但是网络空间战略司令部司令是保障和维护军队信息网络, 以及保护国家网络空间的关键资产、系统和功能的网络空间作战方面的被支持指挥官。

② 战区级军队信息网络运维是那些在一个战区发生的活动——可能影响在该战区的作战行动。作战司令部的联合网络空间中心应与网络司令部网络空间支撑元素进行现场协调, 以确保效应限制在授权范围内。受影响的地理性作战司令部是战区级军队信息网络运维方面的被支持司令部。

③ 战略司令部司令是全球性网络空间作战的被支持司令, 并且在适当情况下, 可把网络空间作战授权给网络司令部司令。

④ 战区网络空间作战的火力和机动的指挥。网络空间作战支持联合部队指挥官的目标, 联合部队指挥官是被支持的指挥官, 军队级网络作战司令部提供必要的支持。联合部队指挥官负责把网络空间作战火力和其他火力整合和协同, 并可以使用任何指定的或配属的资产或提供支持的网络司令部的资产。联合部队指挥官与网络司令部协调自己的需求, 以确保它们在执行中被考虑到和优先安排。当联合部队指挥官的能力正受到攻击, 以至于友好网络空间的一部分被降级、破坏或丢失, 网络空间作战机动将变得很重要。

(3) 大多数进攻性网络空间作战和一些防御性网络空间作战的决策权需要仔细考虑预期效应和地缘政治限制。然而, 一些进攻性网络空间作战和一些防御性网络空间作战活动本身就具备跨区效应, 需要跨部门协调, 排解在网络空间中的活动之间的冲突, 并适当考虑非军事因素, 如外交政策影响。由于这些原因, 进攻性网络空间作战以及一些防御性网络空间作战需要仔细规划、深度情报支持和机构间协调。在全球范围内, 对网络空间的依赖日益增长, 需要仔细控制进攻性网络空间作战, 当采用进攻性网络空间作战时需要获得国家层面的批准。这就要求指挥官了解国家网络政策的变化和对作战授权的潜在影响。

(4) 网络空间的通用作战图有利于网络空间作战的指挥, 以便获得实时的、全面的态势感知。一个网络空间通用作战图应包括快速融合、关联和显示来自全球网络传感器的数据, 提供友好的、中立的、敌对的网络可靠信息, 包括他们的物理位置和活动。此外, 网络空间通用作战图应支持来自各种来源(即军队、情报界、跨部门机构、私营企业和国际伙伴)的实时威胁和事件数据, 提高指挥员的能力——识别、监测、鉴定、跟踪、定位,

并采取行动以响应网络空间活动。

### 3. 网络攻防对抗

网络攻防对抗，是网络空间作战和安全斗争最激烈的部分，主要指针对关系国计民生的国家网络、支撑作战体系的军事网络，综合运用多种手段展开的瘫痪与护网行动。

在网络攻击中，既有利用“网络数字大炮”、分布式拒绝服务等针对互联网系统的攻击，也有利用病毒、木马、后门、漏洞等针对互联网用户的攻击；既有针对有线广域网的攻击，也有针对无线局域网的攻击；既有使用软打击式的攻击，也有使用硬摧毁式的攻击。

网络攻击手段的快速发展，使网络防护一直处于十分不利、困难重重的境况下，加强网络防护，成为世界各国和军事力量的共同选择。尽管在网络全球化带来“一荣俱荣、一损俱损”背景下，全面致瘫网络已变得不可取，但局部致瘫的风险性却在大大增加。无论是国家的战略支撑网络，还是军队的作战体系网络，一旦遭到打击就会造成运转失灵，产生牵一发而瘫全身的严重后果。

因为对手可创建多个连锁效应，可能不受物理地理、民用/军用界限的限制，并极大地扩大需要保护的区域。需要保护的网空间能力不仅包括基础设施（计算机、电缆、天线、交换器和路由设备），也包括电磁频谱的一部分（例如数据链路频率，包括卫星下行链路、蜂窝和无线），还包括内容（数据 and 应用程序），它们都是军事行动所依赖的资源。网空间保护关键在于积极控制部队信息网，监测、侦测和阻止恶意流量进入和发生信息泄露。

防护友好的网空间需要联合使用防御能力和作战安全。因为在网空间中，效应发生快，防护网的自动化技术、核实批准的网络配置、发现网络漏洞通常会比人工措施更有机成功。然而，强大的加密和最安全的网络协议不能防护不受训练/有动机的用户的影响，因为他们不采用适当的安全措施。指挥官应确保人员了解他们的网络安全角色并为自己的行为承担责任。

### 4. 网络实体控制

网络实体控制，是网空间作战最创新的部分，主要指针对国家重要工控系统、战场核心控制网以及物联网等，展开有效的渗透与控制活动。网时代的一个突出表现，就是一切皆在网中，网与实体深度融合，通过网直接操控终端实体，而且这已成为极为普遍的现象。网实体控制的主要途径，是通过系统入侵与病毒预置，达到入侵网、操控对手的目的。

利用网控制对手实体，虽然“小荷才露尖尖角”，但却给人以严重警醒。如不特别防范，未来战略博弈的一方通过网恶意控制，造成另一方金融崩溃、交通混乱、水电停供，以及装备失控、武器失灵等，将不再是天方夜谭。

### 5. 网舆情导控

网舆情导控，是网空间作战和安全斗争最尖锐的部分，主要指围绕网信息的各种传播渠道，争夺舆论主导权进而争夺人心的长期交锋和博弈，也被称为“心灵政治”，



它是传统心理战在网络空间的延伸与发展。网络空间出现后,突破了信息传播的传统格局和多种门槛,各类信息网站、社交论坛、交流平台的涌现,使网络信息产生了实时性、爆炸性、虚假性、发酵性等新特性。例如,任何一条信息都有可能借助发达的互联网演变成轩然大波。近年来,内、外部各种反华势力,无不争相把操控网络舆情作为对我“和平演变”新途径,并已形成相对稳定的运作模式。

网络已经成为社会心理的晴雨表和焦点事件的传播源,成为舆论交锋的主战场、多元文化的角力场、“颜色革命”的试验场。现实世界的全部信息折射到网络虚拟世界,虚拟世界的“一颦一笑”,都将深刻地影响着现实世界。

## 6. 网络价值博弈

网络价值博弈,是网络空间作战和安全斗争最高端的部分,主要体现在“网络自由”与“网络主权”两种不同价值观的冲突上。目前,国际上一些拥有网络技术优势、别有用心的发达国家,推出所谓的“网络自由”价值理念,打着网络无疆、“人权大于主权”的旗号,以期把别的国家网络变成不受约束的飞地,甚至“网络殖民地”。中国等国家则提出“网络主权”价值理念,强调在维护国家主权、保护国家网络安全的前提下,维护个人网络权益,开展网络国际开发合作。

“网络自由”理念貌似光鲜,实则虚伪。以美国为例,对网络的控制就最为严格,如果谁在网上散布恐怖主义、伊斯兰革命,对不起,“FBI”立马会找到你。一些西方大国的所谓“网络自由”,实际上是他可以自由,你则绝对不可以随便。“网络主权”的主张则是国家主权在网络空间的映射,有其实实在的边疆、国防等内容,是世界各国都拥有的一份基本权力。

## 7. 网络规则制定

网络规则制定,是网络空间作战和安全斗争最叫板的部分,主要围绕网络空间管理、利用、军控、安全、冲突等规则制定展开合作与斗争。网络规则制定,关系网络利用的公开、公平、公正,关系网络空间的安全与发展,是一项功在当代,利在千秋的人间大事。

我国必须长远谋划、抢先动作,在维护国家利益的同时,树立负责任的网络强国形象,联合相关国家,建立广泛的国际网络空间规则,制定统一战线,全面参与和推进网络空间国际法律法规的制定。对于美国在法规里把网络攻击等同于战争、试图确立新战争标准的做法,要坚决反对;对于一些国家要求互联网真正实现国际化、弱化美国控制的呼声,要予以支持,同时,提出一系列利于网络安全与发展、利于国家网络主权完整、利于国际网络技术进步的行业和行为标准,营造良性的制定网络规则的国际环境。

## 8. 网络技术比拼

网络技术比拼是网络空间作战和安全最基础的部分,主要包括网络核心技术、网络应用技术、网络管控技术、网络攻防技术的全面较量,并聚焦在电子芯片、传输系统、操作系统、多网融合、安防溯源、应急响应、容灾备份、网络攻击、网络防御等技术发展上。

网络空间作战和安全斗争，没有技术的支持，便是建在沙滩上的楼阁，根基必不牢固，必摆脱不了受制于人的尴尬局面。打破发达国家对网络技术的垄断控制，研发我国自主可控的网络核心技术，打造过得硬的网络产业队伍和培养网络精英人才，已成为我国网络空间斗争不可回避的应急任务和长期任务。在发展网络核心技术、走自主可控道路的同时，也要与闭关锁国、自缚手脚的错误倾向做斗争。技术上的自主可控，是网络信息安全的目标，但不是网络系统建设一票否决的指标。自主不能排斥开放引进，可控也是相对的，要把安全引进与自主可控当作两项并行不悖的长期任务，防止片面用自主可控教条格式化网络和描绘安全，最终走到“自阻难控”的死胡同里。信息时代是广泛联系的时代，是全球一体化的时代，只有站在巨人的肩头上才能摸得更高，实现跨越发展。在发展自主可控的网络技术方面，要始终自觉与崇洋媚外、国门洞开以及不切实际闭关锁国两种倾向作斗争，防止对外来的东西一律捧起或一概棒杀，从一个极端跑到另一个极端，从而走出一条面向世界、以我为主的网络核心技术发展之路。

## 9. 网络服务保障

(1) 保障，就是提供后勤和人员服务，这是维持和延长作战直到成功完成任务所必需的。各军种与支援部队为网络空间作战提供组织、训练、装备的后勤保障。联合部队指挥官必须确定所需的部队和能力、关键的网络空间资产，评估风险，确保冗余性（包括非网络空间替代选择），积极演练连续性作战计划，以对降级或破坏网络空间的访问或可靠性的中断或敌对行动作出响应。

(2) 信息技术不断快速发展，这又需要部队提高开发、装备和维持网络空间能力，适应快速变化的作战环境。联合部队需要具备能力，迅速把新的网络空间功能集成到自己的武器库。此外，联合部队可能需要迅速更新自身的网络，部署新技术方面的压力必须与批准的要求和增加的风险进行平衡，其实现必须精心安排，以防止各军种的网络不融合。

(3) 保障的一个重要组成部分是维护一支训练有素的部队。最成功的网络入侵和攻击可以归因于较差的操作员和/或管理员的安全做法。安全部署的资产只有在得到相应的维护，才能保持安全。

(4) 许多关键的旧系统不容易升级或修补。其结果是许多风险在不同的军事机构发生，这些都是通过信息网络中无法/不能打补丁系统引入的。这种风险可以通过附加网络保护层来缓解，所以附加保护层必须得到维持。另外一些硬件功能也可能随着时间而下降，因此需要部件、软件或固件升级。更换因磨损或敌人发现的、可能攻破的部件是必要的，以确保传感器以及前沿部署的网络空间能力在需要时都准备好了。当必须更换或升级无法实际接触的系统（如部署到远程站点或船舶上的），就会面临重大问题。至关重要的是，指挥官需要明白这些漏洞存在所带来的风险，不只是对自己所指挥的作战行动，而且包括对全军作战任务能否成功带来风险。最后，无论目标作战环境如何改变，不经常访问的应变性软件功能也可能需要定期刷新和重新测试，以确保它们仍然既安全又能够产生所需效应。

### 1.3.4 网络空间作战能力要求

网络空间作战能力是决定作战胜负的关键，对其能力有更高的要求。具体来说涉及以下内容。

- (1) 能操作企业多个级别（从非密到绝密级别）的计算机网络和电信网络。
- (2) 能提供全球链接的企业通信网络基础设施，能提供与联合组织、多国组织、非政府组织可互操作的企业通信网络，从而提供关键战场指挥等能力的端到端接口，确保网络作战支援，确保行动自由。
- (3) 能在驻防和部署作战期间，联合多军种作战网络、友好国家网络和其他规定网络，使得可以通过不同的情报共享关系访问联合作战网络，从而促进有效联合/多国作战，确保行动自由。
- (4) 能定义公私伙伴职责、任务以及权限，以确保各军种或其他特定网络空间自由使用商用频段。能在各个网络作战和关键基础设施与核心资源保护等方面与公、私伙伴共享信息并协作。
- (5) 能提供获取、处理和传递网络作战信息的指挥控制系统能力，便于指挥官的决策，从而形成有效作战。
- (6) 能使全球范围的授权用户提供网络作战接入能力，能汇总连入网络的所有有关信息系统源的数据，以支持分布式的、远程、战场指令现场作战，确保行动自由。
- (7) 能以一种全自动化的实时方式监控网络和信息系统状态，进行系统维护，收集系统历史指令和使用速度。
- (8) 能提供陆海空作战网络和其他规定网络空间的深度防御能力；能实时监控网络威胁事件，并实时汇报；能够实时监控网络侵入和未授权行为；能实时分析并了解网络中的恶意和未授权行为的性质。
- (9) 能防止受到网络和电子攻击，能防止受到网络威胁事件的攻击，与网络威胁事件作战。能在降级网络行动条件下作战，从而实施有效战场指令和作战。
- (10) 能对友方网络、特定网络和敌方网络的行动进行标记，以支援网络作战行动。
- (11) 能提供物理和网络作战保护，防止全谱军事行动的各个阶段期间关键基础设施和关键资源受到致命性的和非致命性的攻击。
- (12) 能确保重要网络作战能力的有效性、保密性和完整性。
- (13) 能形成一个标准的、可分享的地球空间基础，满足所有战场指挥基本信息要求。
- (14) 能创建、更改或分发任务命令（书面和语音两种），包括附加的图形，从而能使指挥塔、平台和领导之间的有效战场指挥通信。
- (15) 能提供演习和培训支持，以便通过能准确代表人物频谱和环境频谱的嵌入式演习和培训工具准备好作战。

## 1.4 网络空间作战环境与作战流程

### 1.4.1 网络空间作战环境

网络空间作战环境是指遂行网络空间作战任务时所处的周围情况和条件的总和。全面了解网络空间作战环境的内容及特点，能动地利用环境，对网络空间作战效能具有重要意义。

根据对网络空间作战的影响程度不同，可将网络空间作战环境大体上分为物理环境、逻辑环境和社会环境。

#### 1. 物理环境

物理环境是网络空间的物质组成及影响因素中的物质系统，是网络空间实施作战的基本依托，包括时空环境、硬件环境和电磁环境。

(1) 时空环境。时空环境是网络空间在陆、海、空、天各维空间所处的时空位置及相关时空条件的总和，包括地理、海洋、天空、太空环境和时间特征。网络设备的空间位置是一国行使网络主权的基础，对网络安全影响重大，如通过攻击电力网能快速造成网络的大面积毁瘫，断开海底光缆接入点能有效断开一国的互联网；电离层是天波传播的介质，影响战场网络的构建与运用；星际互联网成为未来战场网络的制高点；同时，时间成为网络空间的重要维度，实时感知逻辑拓扑、网络信息在时间维度的动态变化，成为网络空间作战的前提和基础。

(2) 硬件环境。硬件环境是支持网络运行的所有硬件、信息基础设施、物理连接器以及监控、维护网络运行的硬件设施的总和，包括终端、嵌入式处理器、网络设备、传媒介质及转换器、输入/输出设施（备）、存储介质和网络监控设备 7 类。智能手机、平板电脑等移动智能终端日益成为远程控制和网络攻击的重要目标；工业、电力、交通控制系统和物联网中的嵌入式处理器成为网络空间作战的重点目标；交换机、路由器等网络设备是网络空间作战的关键节点；海底光缆、主干光缆、骨干光缆是信息网络的关键链路，成为“毁点断链”的重要目标，除可以实施物理打击外，“以软制硬”即用软件打击硬件的手段快速发展；移动硬盘、U 盘、光盘等存储介质可以“摆渡”病毒、窃取秘密。

(3) 电磁环境。电磁环境是网络空间及其周围一定空间内所有的电磁辐射共同形成的环境，包括网内电磁环境和网外电磁环境。电磁环境是物理环境中的能量层，也是信息环境中的信号部分，具有贯通陆、海、空、天战场的特性。网内电磁环境，就是网络用频谱设备构成的电磁环境，作为信息载体的电磁信号可能被干扰，也可能被敌方键盘、显示器和电力线信号监测装备监听。网外电磁环境，是当前复杂电磁环境中影响网络空间的部分，

分为人为电磁环境和自然电磁环境。电磁环境对于网络的运行和攻击具有重要影响。可以运用电子战、网电一体战的手段，对网络电磁信号实施监听、干扰、欺骗，甚至对网络电磁设备实施“硬摧毁”。

## 2. 逻辑环境

逻辑环境是维持网络空间运行的逻辑连接关系、软件和数据总和，是实施网络空间作战的主要战场环境，包括拓扑环境、软件环境和数据环境。

(1) 拓扑环境。拓扑环境是计算机和网络设备间逻辑连接关系的总和。逻辑拓扑与实体拓扑共同构成网络拓扑。实体拓扑相当于交通路网，表明“有什么路”，相对固定；逻辑拓扑相当于行车路线，表明“路怎么走”，处于不断变动之中，反映了网络的实时链接情况和信息的流向流量，逻辑拓扑动态感知是网络空间态势感知的重要内容。

(2) 软件环境。软件环境是支持网络运行和实现网络应用的各种软件的总和，包括终端操作系统、网络操作系统、网络通信协议、应用软件和网络管理软件。如主流计算机操作系统有微软公司的 Windows 系统、美国电话电报公司的 UNIX 系统等。手机等移动智能终端主要使用谷歌公司安卓 (Android)、微软公司 WP (Windows Phone) 和苹果公司操作系统 (iOS) 三大操作系统。主流网络操作系统是思科公司 (Cisco) 的 IOS 和 Novell 公司的 NetWare 网络操作系统，操作系统被外国公司垄断，对网络安全构成重大威胁。网络通信协议主要有传输控制协议 (TCP, Transport Control Protocol) / 网际协议 (IP, Internet Protocol) 和非 TCP/IP 协议，基于互信前提开发的 TCP/IP 协议是当前网络空间两大漏洞之一。应用软件是所有软件中种类最多的，如微软公司的 Office 系统、腾讯公司的微信等。专门用于网络安全的应用软件自身也是不安全的，如防火墙、防病毒软件、反黑客软件都存在大量漏洞，常见的木马、病毒和钓鱼软件本质上也是应用软件。网络管理软件，如 HP 公司 OpenView、IBM 公司 Tivoli NetView 等。当前，云计算、虚拟网络技术构成了更加复杂的软件环境。据统计，平均每 1000 行计算机程序代码中就有 15~20 处错误，存在巨大的软件漏洞。

(3) 数据环境。数据环境是由数据类型、结构和相关数据活动构成的环境。数据是网络空间的核心资源，随着电子商务、物联网等网络应用的日益广泛，网络数据量急剧增加，数据非结构化特点更加突出，催生了“大数据”概念。大数据存储、挖掘、分析技术得到了快速发展，大数据与云计算结合使异质异构异源数据处理成为可能，给信息融合、抽取和应用带来了革命性的变化。当前，数据泄露、损坏、丢失、淹没、窃取、篡改、非法访问、非法使用等针对数据的安全事件日益频繁，信息面临着保密性、完整性、认证性、不可否认性、可控性和可用性等方面的严重安全威胁。

## 3. 社会环境

社会环境是影响网络空间活动的物质和精神条件的总和，是网上网下亿万用户虚拟交互形成的具有亚社会性质的虚拟环境，包含网络政治、经济、军事、外交、人文环境等。网络类型与规模、用户数量与构成、网络服务与安全等是衡量网络社会环境的重要指标。

网络空间既像人民参政的城市广场，也像人们购物的商业大街，又像潜藏罪恶的阴暗小巷，还像间谍窃取经济军事情报的秘密通道，更像一个战场。虚拟空间与现实社会的密切联系，为网络空间作战提供了越来越多的可能。

(1) 网络政治环境。各国大力推进政府上网工程，电子政务日益普及，网民参与政治热情高，西方国家扩大与其他国家的“数字鸿沟”，利用网络传播的非对称优势，控制国际网络媒体，争夺网络话语权，挑起“网络冷战”，策动“颜色革命”，给世界政治格局带来了新的变量。

(2) 网络经济环境。关键信息基础设施成为国家的重要经济支撑，知识经济逐步网络化，信息服务、网络媒体、网络购物、网络游戏、网络娱乐、支付宝、余额宝等构成网上经济的主要内容。网络新兴产业给传统产业模式和经济安全带来了严峻挑战。以计算机和网络技术为代表的国家科技水平成为国家安全的重要因素，如被称为“八大金刚”的美国思科、IBM、谷歌、高通、英特尔、苹果、甲骨文和微软等网络企业，对我国网络空间安全构成了严重威胁。

(3) 网络军事环境。国际互联网、移动通信网和战略指挥信息系统等构成战略网络，指挥控制网、战场通信网、预警探测网、卫星通信网、导航定位网和战术数据链网等构成战场网络。目前，美军 95% 的军用网络都已经接入互联网，并在互联网部署网络部队和网络武器，网络犯罪、网络黑客和网络恐怖主义频发，军队网络化和网络军事化进程加速，对现代战争影响巨大。

(4) 网络外交环境。外交已不是国家与国家、政府与政府之间的专利，在国家、国际组织为主体的传统外交模式基础上，网站外交、网民外交新模式日趋活跃，谷歌、推特、脸谱等形成领域垄断，在幕后国家和资本推动下，操控网络舆论，对网络主权和信息主权造成严重侵害。

(5) 网络人文环境。一方面，网络给人类提供了一个更加开放、多元的交流平台，微博、微信、网络社区、虚拟社会日趋活跃，网络认知和舆论环境成为重要构成要素，网络舆论渗透到网上网下各个领域，成为国际国内政治生态“风向标”；另一方面，英语等优势语种在操作系统、应用软件、门户网站等方面占据统治地位，西方国家加紧推行网上文化扩张和“文化殖民”，给文化安全带来了巨大冲击。

#### 1.4.2 网络空间战场的组成

网络空间战场是由参与网络空间作战行为的多个方面的资源组成的，如图 1-7 所示，主要分为以下五个部分：网络战场环境，网络空间数据，网络空间作战武器，网络空间作战技术，网络空间作战力量。

网络战场环境是网络空间作战开展所需要的基础设备的依托，包括信道传输媒介、通信网络、终端设施、路由设备等。目前主要的网络战场环境有全球网络环境、国家网络环境和军事网络环境。全球网络环境是由全球众多网络互联而成的全球互联网。国家网络环

境也可称为国家信息基础设施,如中国科技网、中国教育网与科研网、金桥网、中国公众互联网等骨干网络。如果国家骨干网络被敌方瘫痪或者控制,将严重影响社会的正常运转。军事网络环境是国家军事力量管理和指挥的神经系统。军事网络与民用网络不同,对其的破坏或者在其中对军事机密的窃取有可能直接改变战争的进程。因此,各国对于军事网络的防御也是最为严格的,采取物理分离、严格接入管理等办法防止对军用网络的攻击事件的发生。

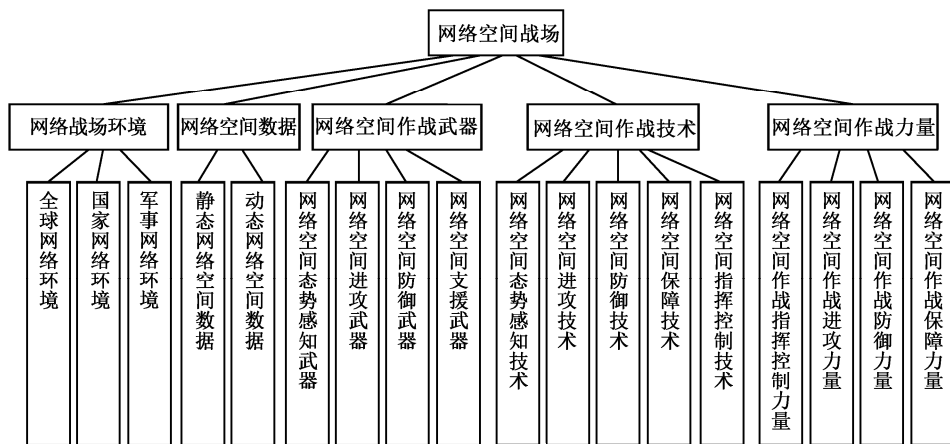


图 1-7 网络空间战场组成

将网络空间数据作为网络空间战场的一部分是考虑到数据是网络空间作战的能量,是网络空间作战行动实行的依托。网络空间数据是指为了快速、高效地进行网络空间作战行动,需要掌握网络空间运行的态势数据。数据按时效可以分为静态网络空间数据和动态网络空间数据。静态网络空间数据是指对各种知识的存储和积累,为使用者提供查询服务,如网络的结构数据、各种法律、体制文档等。动态网络空间数据是指网络空间运行的实时状态数据,如网络探测数据、入侵报警数据、流量数据等。这些数据对于掌握网络战场的状态,抢占网络战场制高点都有着重要的意义。

网络空间作战武器是实施网络空间作战的基础。按照不同的标准对于网络空间作战武器有着不同的划分。按形式可以分为软件武器和硬件武器;按作战运用级别可以分为战略级网络空间作战武器、战役级网络空间作战武器和战术级网络空间作战武器;按功能可以分为网络空间态势感知武器、网络空间进攻武器、网络空间防御武器和网络空间支援武器。目前,在网络空间作战武器的研究中,按功能划分武器较为普遍。

由于网络空间作战是高技术行动,技术对于网络空间的影响是全方位的。进行网络通信需要通信技术,进行数据交换需要数据交换协议技术,进行网络空间态势感知需要数据采集、融合、分析技术,进行作战需要网络空间攻防技术。是否掌握先进的网络空间作战技术对于网络空间战争胜负有着重要的影响。网络空间作战技术包括网络空间态势感知技术、网络空间进攻技术、网络空间防御技术、网络空间保障技术和网络空间指挥控制技术。

网络空间作战力量是指具有网络空间作战技术的作战人员。战斗员作为网络空间作战行动和进行决策的操作者，网络空间作战力量也是网络空间战场的一个重要组成部分。由于网络空间作战力量是指接入网络空间的战斗人员，因此作为网络标识的 IP 地址、邮箱等信息是网络空间作战力量的一种属性信息。一个人员可以拥有多个 IP，但是每个 IP 都对应网络空间中的一个角色，这时一个人员在网络空间中就可以拥有多个角色。按照职能网络空间作战力量可以分为网络空间作战指挥控制力量、网络空间作战进攻力量、网络空间作战防御力量和网络空间作战保障力量。

### 1.4.3 网络空间作战的过程

#### 1. 网络空间作战基本形式

网络空间作战的本质是一个双方攻防对抗的作战形式。网络空间作战的胜败取决于双方网络体系的对抗。图 1-8 是网络空间作战的基本形式。

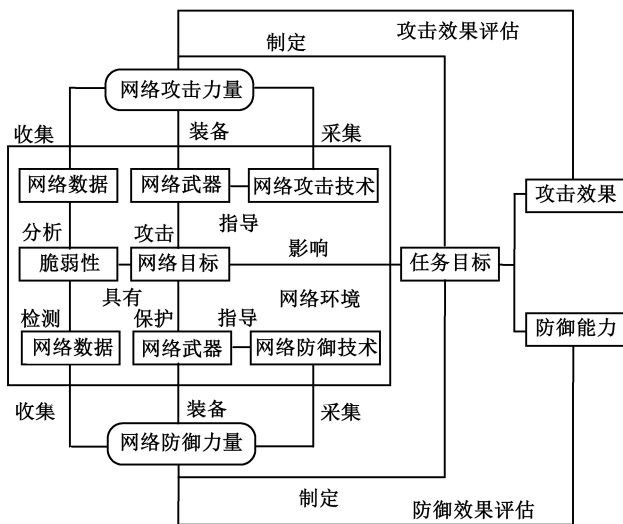


图 1-8 网络空间作战的基本形式

网络空间攻击和防御力量应用网络攻防技术，收集网络中相对脆弱的数据，通过网络武器对网络目标进行攻击和防御。之后，网络空间攻防力量对于其制定的网络作战任务目标进行评估，对网络作战的效果进行反馈并制定下一步作战计划。由此模型可以看出，网络空间作战中网络空间力量需要掌握网络数据收集情况、网络装备信息、网络技术能力、网络环境信息、任务完成情况等信息。



## 2. 网络空间作战的过程

网络空间作战的过程可用图 1-9 来描述。在网络攻击行动中，战前准备包括目标信息收集和锁定、目标弱点的探测和挖掘两步。网络攻击的前期准备需要对目标信息全面的收集并分析其攻击的可行性，如网络 IP 地址的范围、拓扑结构、防火墙设置；目标网络的操作系统类型即版本；DNS 服务器、邮件服务器以及其他相关服务器的注册信息；目标网络开放的端口信息、服务信息；到达目标网络的路由信息、服务器信息等。获取这些数据是进行攻击的基础。之后，通过分析收集到的信息对目标的各种漏洞进行分析挖掘，如系统服务漏洞、应用软件漏洞、弱口令等。网络防御行动中，战前准备主要是对弱点的扫描分析并进行修补、对网络中异常行为的探测、访问控制、入侵行为检测等预警行动。

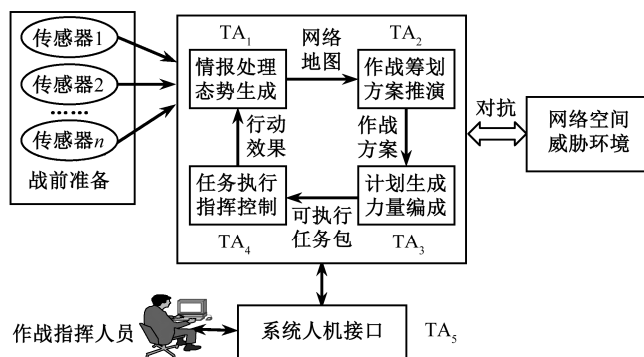


图 1-9 典型网络空间作战过程

战前准备后开始战斗过程。在战斗过程中，从情报处理与态势生成、作战筹划与方案推演、计划生成与力量编成、任务执行与指挥控制和系统人机接口交互 5 个典型作战行动阶段出发，需要重点突破的 5 个技术体系，标记为  $TA_1 \sim TA_5$ 。其中技术体系  $TA_1$  是将收集的数据转换为适合情报生成的信息格式，生成战场态势图，提供支撑整个作战过程的网络地图和基础设施；技术体系  $TA_2$  是辅助指挥员开展作战筹划，通过方案推演和效果分析优化作战方案的技术应用；技术体系  $TA_3$  形成具体行动计划，将网络作战力量要素制作成可执行任务包；技术体系  $TA_4$  是部署作战平台，开展行动指挥控制，完成作战任务的技术应用，达到作战应该达到的行动效果；技术体系  $TA_5$  是实现高效人机接口的技术应用，实现以人为的前提下人机系统的高效协作。面临网络威胁环境，及时开展作战行动和网络对抗，争取最好的作战机会并取得胜利。

以上 5 个作战行动阶段对应的技术体系和关键技术见表 1-1。可以看出，5 个技术体系的研究内容主要涉及网络空间作战三大要素，以及将这些要素集成到网络空间作战行动中的关键技术，而不涉及对网络空间传感器和作战能力集中的接入、功能（攻击、防御等）及通信技术投入。

表 1-1 网络作战阶段与技术体系和关键技术对应关系

作战阶段	对应的技术体系	对应的主要关键技术
情报处理 态势生成	系统体系结构 (TA <sub>1</sub> ) 直观界面 (TA <sub>5</sub> )	网络作战情报处理 (大数据处理) 网络空间态势生成 (客观态势) 网络作战系统体系结构设计 网络作战系统基础设施构建 大规模并行图形处理
作战筹划 方案推演	网电战场空间分析 (TA <sub>2</sub> ) 直观界面 (TA <sub>5</sub> )	网络作战计划辅助生成 网电作战兵棋推演
计划生成 力量编成	任务生成 (TA <sub>3</sub> ) 直观界面 (TA <sub>5</sub> )	高级编成语言形式化分析 网络作战任务包生成 网络作战预案生成
任务执行 指挥控制	任务执行 (TA <sub>4</sub> ) 直观界面 (TA <sub>5</sub> )	脚本运行环境构建 支撑平台构建
系统人机接口	直观界面 (TA <sub>5</sub> )	网络作战系统用户界面

## 1.5 网络空间作战与其他作战之间的关系

### 1.5.1 网络空间作战与电子战的关系

随着无线和光学技术的发展, 计算机网络和通信网络趋于融合, 网络空间也越来越依赖电磁频谱, 电磁频谱成为网络空间的关键支柱。电磁空间是由各种电磁场和电磁波组成的物理空间, 电磁频谱是该空间所有行动的媒介。可以看出, 电子信息系统首先存在于电磁空间, 而电子战是战场指挥员取得制电磁频谱权的主要途径。因此, 虽然网络空间作战和电子战在实体、原理和技术上有很大的不同, 但二者却有着密切的关联。

网络空间最早的定义是指计算机网络空间, 随着认识的不断深入其概念已经发展到涵盖所有电磁频谱和电子系统的物理领域。当多个电子信息系统通过电磁波相互连接形成网络时就构成了网络空间。因此, 网络空间是网络化的电磁空间, 必须高度依赖于电磁空间, 以电磁空间为基础。电磁空间的物理基础是工作在电磁频谱中的任何电子信息系统, 它们不一定要形成网络。与网络空间概念相比, 电子战逐渐成为战场制胜最为重要的因素之一。目前, 电子战已经从最初单一的无线电通信对抗发展为包括雷达对抗、通信对抗、光电对抗、战场信息网对抗以及其他电子对抗在内的综合电子对抗。显然, 随着网络空间相关技术的发展, 传统的电子战方法和应用也将随之改变。

## 1. 电子战是网络空间作战的重要内容，并起着关键作用

(1) 电子战是接入敌方战场网络空间的主要途径。网络作战依靠电子战实现对电磁频谱的控制和自由接入。接入敌方网络空间是实施网络空间作战的前提，在接入敌方无线网络时需要借助电子战设备帮助，如美军的电子战飞机都要求具备网络作战能力。尤其战场网络空间，一般是一个封闭或半封闭的网络体系，如美国陆军陆战网、美空军指挥控制星座网，还有其他物理隔离的指挥控制网络和防空系统，如战场雷达防空网、地域通信网、目标监视网、火力协同网、指挥控制网等，这些网络所构建的信息空间远远超出了计算机网络的范畴，它们并不直接与因特网相连，对其进行攻击时，首先面临的的就是信号接入问题。电子战正是解决这一问题的基础，军事作战网络包括大量无线接口和链路，以及开放式传感器，通过电子战技术以电磁波形式从天线口面或其他节点进入敌战场网络空间是最为可行的途径。换言之，网络空间作战的作战效能将主要通过电子战手段以电磁波的形式传递到敌方战场网络空间。而且通过电子战手段，还可以对敌网络空间实施硬摧毁、干扰压制等行动。

(2) 战场网络空间的物理层侦察和攻击主要依靠电子战技术。对于战场网络空间而言，其物理层信息主要包括各个节点，以及信息链路的地理位置和工作参数，计算机网络对于这些信息的获取无能为力，只能依靠电子战技术和装备。同时，随着反辐射打击、定向能等高新技术的发展，电子战已具备很强的实体打击能力，可有效破坏敌方网络空间物理基础设施。

(3) 传统电子战手段已具备一定的网络空间作战的能力。电子侦察可以对敌战场网络空间的节点（例如各种辐射源）进行精确定位和参数测量，从而实现了网络空间物理层态势感知的部分功能；压制式电子干扰可以降低敌网络空间获取外界信息的能力及扰乱敌方信息网络的正常运行；逼真的欺骗干扰则可将错误或虚假信息引入敌方信息网络，达到信息欺骗、影响指挥人员决策判断的效果；完善的电子防御则可以阻止敌方通过电磁频谱接入己方网络空间并实施攻击和破坏。

(4) 电子战装备将是未来网络空间作战的主要平台。从美军相关研究项目的报道不难看出这样的趋势。美空军“舒特”项目的网络电磁攻击武器集成于 EC—130 电子干扰飞机的干扰设备之中，而美国海军的“下一代干扰机”也集成了网络电磁攻击能力。因此不难推测，电子战装备将是搭载各种网络空间武器的主要平台。

(5) 电子战技术的进一步发展将支撑形成完备的网络空间作战能力体系。多维全域电子侦察、信道编码识别、网络拓扑分析、通信协议分析与识别等新型电子侦察技术的发展将支撑网络空间态势感知能力形成；精确电子战、反辐射打击、定向能、组网协同电子战、基于协议的电子信息攻击、恶意代码无线注入等新型电子攻击技术的发展将支撑网络电磁攻击能力的形成；低截获/低检测信号设计、低旁瓣天线、信号加密等电子防护技术的发展将为反网络空间探测攻击把好第一道门，极大地增加敌方从“信号层”跨入“信息层”的难度；而电磁频谱控制技术将增强战场电磁频谱规划、协同和管理能力，从而有效地保障战场网络空间的建立、维护，以及顺利地通过电磁频谱接入敌

方战场网络空间实施作战。

电子战是网络空间作战的主要手段之一，也是进入并有效控制敌方网络空间（尤其是战场网络空间）的必要前提。

## 2. 网络空间作战与电子战之间的相互关系

对于二者之间的关系问题，一种观点认为电子战应完全纳入网络空间作战，而另一种观点则认为电子战不应完全纳入网络空间范畴。虽然把电子战完全纳入网络空间作战的做法有一定的道理，但是第二种观点更具有充分的理由。电子战与网络空间作战的相同点可列举为：均需以电磁频谱为媒介；均依赖于精确的电子信息和情报支持；面对的对象都是信息系统；均可以通过技术欺骗影响对手。而电子战与网络空间作战的不同点可列举为：前者无须联网，而后者以网络为物理基础；前者不以网络为作战目标，后者以网络为中心；后者网络战的概念与前者概念差别很大；前者对信息环境产生影响，而后者可作用于硬件、软件和数据成员；网络空间要利用一些电子资源，但电子战还服务于陆、海、空、天等其他作战领域，在这些领域内，也需要实现电磁频谱控制。电子战的作战任务明确、清晰、成熟，而网络空间作战任务隐蔽、偶然、突发、模糊、不确定，对目标难以发现和控制，对目标实施进攻还不是很成熟。通过上述对比可以看出，电子战并不能够完全归属于网络空间作战。以通信电台为例，一部电台不能构成网络空间，只有当多部电台相互连接构成通信网时，才具备了建立网络空间的物理基础。

网络空间各部分与实体基础设施、电子系统及部分的电磁频谱相连接，并受到它们的支持。随着新系统和基础设施的发展，它们有可能会使用电磁频谱的增加部分，并具备更高的数据处理能力和速度，而使用的带宽也会越来越大。系统同样还可以设计用来改变频率以及操纵数据。因此，在网络空间中存在物理操纵空间。

### 1.5.2 网络空间作战与网络战之间的关系

在军事理论界，常有人将网络空间作战等同于网络战（Network War），实则不然，网络空间作战是泛指网络空间的作战行动。网络战则是在网络上展开的攻防行动。

国内对于网络战的理解有多种观点，主要可以概括为三种观点：

- （1）“争夺说”，认为网络作战是在网络环境中，以计算机为中心，进行信息侦察、传输、反探测、欺骗和攻击等活动，其目的是争夺制信息权。
- （2）“程序说”，认为网络作战是依靠病毒和软件等计算机应用程序进行的作战行为。
- （3）“攻防说”，认为网络作战是关于保护己方网络，破坏敌方网络系统的科学和技术的学科。

理清二者间的关系应从网络空间作战与计算机网络作战这个角度出发：

一是网络战是网络空间作战军事行动中的重要组成部分。网络战是基于计算机网络信

息的传输、存储、处理和输出等信息行为进行的行动，是网络空间作战的基本形式。网络是信息传播的重要途径，而且计算机网络是建立在数据通信基础之上的。

二是网络空间涉及的范围更广。网络空间主要由电磁频谱、电子系统以及网络化基础设施三部分组成。美国前空军参谋长迈克尔·莫斯利曾开玩笑说，网络空间囊括了从“直流电到可见光波”的一切东西，其范畴已经远远超出了传统意义上的“网络”，而且还包含了一些传统意义上“网络”中所不能包含的元素。随着网络中心化作战的不断发展，战场网络的种类不断增多，作用不断增强，如雷达防空网、地域通信网、目标监视网、火力协同网和指挥控制网等，这些网络所构建的信息空间远远超出了计算机网络的范畴，但从网络空间含义中可看出，这些网络都属于网络空间的范畴。

三是网络空间作战的手段更为多元。它包括的不仅仅是数字信号的计算机网络系统，还有使用各种电磁能量（红外波、雷达波、微波、伽马射线等）的所有物理系统，还涉及电子战和计算机网络攻防战。由于因特网的重要性及其可影响国家安全的明显弱点，大量的网络化系统并不直接与因特网相连。许多军事指挥控制网络和防空系统是隔离或封闭的，外界无法直接访问。然而，对于这些没有直接和因特网连接的网络，也可利用电磁能量进入或实施攻击，达到窃取信息和破坏硬件的目的。这些系统恰恰是必须保持高度警觉的战略系统，利用网络空间对这些战略系统实施攻击，可实现和直接打击相同的作战效果。

四是网络空间作战的效果更为直观。计算机网络作战是以计算机为平台实施的网络攻击与网络防御等行为，作战对象是敌方的政治、经济、金融、军事等关键网络系统，人员直接伤亡较少，具有“兵不血刃”的特点。而网络空间是处于电磁环境中的一种物理领域，因此在网络空间中的战斗并非创造虚拟效果或在某种虚拟现实攻击敌人，而是物理作战，将产生非常真实的作战效果，通过网络空间内的战斗，敌方人员可因此死亡或受伤，影响敌方定位部队、指挥控制，甚至火力攻击的能力。

尽管网络空间中的网络相互依存，但也有少部分是孤立的，这些孤立主要是通过协议、防火墙以及与其他网络物理隔离的形式而存在。例如，像保密因特网协议路由器网之类的机密网络并不会一直与互联网硬线连接，而是借由安全站点进行连接。再加上，一些硬线连接网络的结构会使得他们置身于绝大多数的无线电频率的干扰之外。这些因素促使了这些网络在网络空间中显得孤立，不过还是允许受控连接到全球网络的。

### 1.5.3 网络空间作战与信息作战之间的关系

网络空间作战涉及使用网络空间能力，创建支持跨越物理域和网络空间的作战行动之效应。信息作战只是一系列能够在网络空间或其他领域中执行的作战行动。网络空间作战则可以直接支持信息战，并且非网络下的信息战也能影响网络空间作战。信息作战具体涉及在军事行动中集成使用与信息相关的能力，与其他作战配合，影响、破坏、损坏敌人和潜在对手的决策，同时保护自己。因此，网络空间与信息紧密相关，如军事信息支援作战或军事欺骗，可以使用的媒介等。然而，信息作战还采用物理域的能力实现其目标。从总

的作战目的上讲，两者都是为了夺取并保持战场制信息权，信息作战要服从和服务于联合作战的大局，网络空间作战则要服从和服务于信息作战的大局。

尽管一些网络空间作战可以支持信息作战目标，其他网络空间作战将支持攻击目标，或支持物理域中的作战以实现目标。这种关系既对信息作战来说是一种变革——从功能集中转变到关注对手的一个更广泛的集成功能集，又对网络空间作战来说是一种变革——从基础性的计算机网络作战演变成一种把网络空间作战集成到联合作战中的方法。网络空间作战被认为是信息作战的一个子集，是信息作战的重要组成部分，是信息作战发展到一定阶段的一种重要作战样式，包括了网上情报战、网上电子战、电磁战、网上心理战、计算机网络作战、计算机网络攻击、计算机网络防御、计算机网络刺探、进攻性网络空间作战、防御性网络空间作战和军队信息网络运维等内容；而信息作战可以涉及网络空间的更多信息，可以不在网上就可以展开作战。

#### 1.5.4 网络空间作战与机动作战、火力作战之间的关系

机动作战与火力作战是机械化战争形态中的主要作战样式，战争形态的发展必然导致战争手段更新换代。因此，在战争形态由机械化战争向信息化战争发展过程中，网络空间作战与机动作战、火力作战之间共同成为现代战争的重要作战样式。

##### 1. 网络空间作战与机动作战、火力作战之间的联系

一是从实质上看，网络空间作战与机动作战、火力作战都是现代战争中的重要作战样式，其作战的共同目的都是为了夺取战争的胜利。三者相辅相成，相得益彰。

二是从内容上看，三者之间互有交叉，网络空间作战中包括硬摧毁和软杀伤。其中硬摧毁也可通过机动作战、火力作战来达成。

三是从作战效果上来看，机动作战、火力作战的主战武器，如飞机、坦克、火炮等的核心部位都装备或嵌入有计算机设备、信息控制设备；而网络空间作战的作战效果可直接或间接地支援和保障机动作战、火力作战来达成作战目的。

##### 2. 网络空间作战与机动作战、火力作战之间的区别

一是作战的直接目的不同。网络空间作战的直接目的是夺取制网络权；机动作战与火力作战的直接目的通常是夺占某个地域或歼灭某部敌人。

二是作战的空间不同。网络空间作战的战场空间是在网络空间上实施各种作战行动；机动作战与火力作战通常是在有形的物理空间实施各种作战行动。

三是主要作战手段不同。网络空间作战的主要手段是以信息为基础，运用黑客攻击、病毒入侵、预置破坏性程序、电磁脉冲炸弹破坏等手段达成作战目的；机动作战与火力作战是以机动力与火力为基础，运用兵力攻击、火力摧毁等手段来达成作战目的。

# 第 2 章

## 美国网络空间作战 战略和指挥控制体系

美国是一个信息化程度非常高的国家，可以说，网络空间已经嵌入到了美国社会的每一个细胞，已成为美国经济的一个关键领域，成为创业、技术进步、言论自由传播和新型社会网络的新型孵化器，推动着美国经济的发展。美国政府认为网络空间具有高度的战略价值——经济上和军事上的。美国政府下了坚定的决心，分配了充足的人力物力，积极采取行动，制定网络空间的“游戏规则”，获取网络空间的主动权，重塑和主导全球网络空间。

### 2.1 美国网络空间作战战略分析

#### ■ 2.1.1 美国网络空间的战略基础

如果说美国是现在世界上唯一的超级大国，那么在网络世界，美国的优势地位也是超级的。美国在网络空间的优势和对互联网的控制是立体式的、全方位的。

在核心技术上，美国拥有思科、IBM、谷歌、高通、英特尔、苹果、甲骨文、微软掌握互联网关键及核心技术的“八大金刚”。其中，英特尔公司垄断芯片制造，苹果公司称

霸手机与平板电脑等网络终端及操作系统，IBM 在高端服务器等计算机与网络服务上处于领先地位，甲骨文主导商业软件，微软控制国际主流的计算机操作系统，谷歌则拥有世界上最强大的搜索引擎以及一流的研发创新能力……美国的互联网信息技术公司不仅引领着互联网服务的供给，更决定了互联网发展的需求与使用。与此同时，美国互联网巨头在技术创新方面也保持着强大的动力，持续引领全球网络技术业务创新的潮流。如云计算、大数据、虚拟化等这些代表当前互联网时代最为时髦的概念和词汇，都是由硅谷巨头们率先提出和应用的。另据媒体报道，包括谷歌、苹果、IBM、甲骨文、思科、微软、英特尔等在内的美国科技巨头，已宣布成立一个工作小组，其中一项重要的工作就是要在全球的技术创新中，不断建立美国可以主导的技术框架和技术标准。而从互联网架构的顶层意义上来判断，如何在整个互联网技术发展的轨迹上建立独立、超前的技术框架，如何提出先进、实用、与众不同的技术标准，已经成为当前互联网时代最为核心的课题。这一课题相比弃用哪家的服务器、哪个操作系统或哪个软件来说，更具有战略意义。

美国坚决把持全球互联网的域名解析权。互联网的域名是对应互联网数字地址的层次结构式网络字符标志，是网络世界的门牌号，具有唯一性和排他性的特点。由于域名与企业名称、商品标志或商标紧密相连，美国可以从中谋取重大经济与战略利益。美国为维持其域名控制权，2005 年 11 月，在突尼斯召开有关互联网问题的会议上，时任国务卿的赖斯专门写信给当时的欧洲轮值主席，要求他支持互联网名称与数字地址分配机构(ICANN)管理互联网。美国国会还以 423 票对 0 票通过决议，要求美国政府控制互联网。

美国掌握着全球 IP 地址的分配权。在网络世界，IP 地址的多寡犹如现实世界中一个国家地理版图的大小。由于美国控制了 IP 地址的分配，它将绝大多数的 IP 地址留给本国及其盟国的公司和民众使用，其他国家只能分得一点残羹冷炙。例如，中国虽是网络大国，但第 4 版 IP (IPv4, IP version 4) /第 6 版 IP (IPv6, IP version 6) 的地址和域名是从美国租借来的，严重受制于人。

美国还把互联网根服务器控制在自己手里。由于域名解析系统的管理模式呈根状分布，因此根服务器在域名管理中起着决定性作用，哪个国家控制根服务器，这个国家就会在互联网领域拥有巨大权力。目前全球共有 1 个主根服务器和 12 个副根服务器。放置在美国弗吉尼亚州杜勒斯市的主根服务器由美国的 VeriSign 公司负责管理。12 个副根服务器中，有 9 个放置在美国，美军方使用 2 个，美国国家航空航天局使用 1 个。另外 3 个副根服务器放置在英国、瑞典、日本这些美国盟友手里。换句话说，美国拥有对根服务器的直接和间接控制权。只要美国愿意，只需将根服务器与二级域名服务器断开，美国便可瘫痪某个与之敌对的国家互联网系统。2004 年 4 月，利比亚顶级域名“.ly”被封，利比亚便在互联网上消失了三天。2009 年，应美国政府要求，微软公司曾切断古巴、叙利亚、伊朗、苏丹和朝鲜五国的微软网络服务，导致这五个国家的微软网络用户无法登录该即时通信系统。2014 年 1 月 21 日，中国互联网出现罕见的公共安全事故，全国约 2/3 的网站域名服务器解析失败。据粗略估算，受影响的国内用户超过 2 亿，平均受影响时间约 3 小时左右。分析发现，这次事故是由于全球两个根服务器遭到污染，使中国国内通用顶级域的根域名服务器出现异常，由此导致大量网站无法正常访问。



### 2.1.2 美国的国家战略重点

美国网络空间安全总的战略重点是：在保护现有关键信息基础设施的同时，定义和倡导身份标识生态系统，充分挖掘网络空间潜力，采用先发制人的策略，建设未来更为强大的网络生态系统。

#### 1. 战略重点关注领域

美国战略重点关注领域是保护关键信息基础设施。重点关注网络生态系统中软、硬件设施，减少信息基础设施面临的威胁，确保其具备快速反应能力和网络安全信息共享能力，以及增强其快速恢复能力是保护信息基础设施的最佳途径。如果能够证实关键信息基础设施的所有者和经营者能够妥善管理风险，信息基础设施能够确保安全，那么美国政府才认为关键信息基础设施得到了切实有效的保护。当符合下列条件时，网络生态系统才是安全的：

- (1) 用户能够充分认清、掌握和管理信息和通信技术风险；
- (2) 机构和个人能够按规定执行安全和隐私条令；
- (3) 个人、机构、网络、服务和设备满足网络安全标准；
- (4) 信息和通信技术具备安全的通用性；
- (5) 接近实时的端对端协作，能够对网络安全事件发出警告并自动做出反应。

要建设好网络生态系统，美国政府认为需要增强个人与组织安全使用网络的能力；开发和使用值得信赖的协议、产品、服务、配置及架构；建设合作型网络社区以及确保进程透明。

#### 2. 定义和倡导一种支持可信网上环境的身份标识生态系统 (Identity Ecosystem)

美国发布的《网络空间可信身份国家战略》，计划用 10 年左右的时间，通过政府推动和产业界努力，建立一个以用户为中心的身份生态体系。

身份标识生态系统是一个在线环境，其中的个人、组织、服务和设备可以相互信赖，因为有权机构建立的隐私保护和认证它们的数字身份。身份标识生态系统能够保证：

- (1) 安全性，使对手更难以破坏网上交易；
- (2) 方便带来效率，个人可以选择不用像今天一样管理众多的密码或账号；对私营部门，也能从中受益，减少基于纸面的管理流程和账号管理流程；
- (3) 易用性，尽可能使用自动化身份标识解决方案，立足操作简便、耗费最少培训的技术；
- (4) 用户信心，数字身份得到充分的保护，从而提高使用互联网作为各类网上交易的平台；
- (5) 个人隐私，他们信赖他们的数据被负责任地处理，他们会被经常告知谁在收集他们的数据以及用途情况；
- (6) 更多的选择，身份标识证书和设备是由采用可互操作平台的供应商提供的；

(7) 创新的机会，服务提供商开发或扩大所提供的网上服务，尤其是那些具备固有风险的服务。

为确保身份生态体系的建立，明确了4项任务和目标：一是制定身份生态体系框架，细分任务包括建立隐私保护机制，建立基于风险模型的身份鉴别和认证标准，界定参与者的责任并建立问责机制，建立指导小组对制定标准和认证流程进行管理；二是建立和实施身份生态体系，建立和实施身份生态体系互操作基础设施；三是增强用户参与身份生态体系的信心和意愿；四是确保身份生态体系的长期运行和可持续性。

提出了9项高优先行动。这些行动奠定身份标识生态系统实现的基础，行动包括：

行动1：指定一个联邦机构，领导公共/私营部门与实现本战略目标有关的努力；

行动2：制定一个共享、综合的公共/私营部门实施计划；

行动3：加快与身份标识生态系统相符的联邦服务、试点系统和政策进展；

行动4：公共/私营部门配合以实现增强的隐私保护；

行动5：协调风险模型和互操作性标准的开发与精细化；

行动6：解决服务提供商和个人的责任担当；

行动7：在所有利益相关者中开展推广和意识培养活动；

行动8：继续加强国际合作；

行动9：利用有效方式推动全面采用身份标识生态系统。

联邦政府继续作为设想中的身份标识生态系统主要推动者、最先采用者与主要支持者。联邦政府将不断地与私营部门、州、地方、郡以及各国政府合作，提供必要的领导和激励措施，使身份标识生态系统成为现实。

### 3. 挖掘网络空间潜力的作战战略

《网络空间作战战略》是美国国防部推出的首份关于网络空间作战的战略文件。着重阐述了美国网络空间利益及军事行动的全球性，明确了美军网络空间行动的方向和准则，提出5项战略倡议，为其在网络空间领域有效地运行、捍卫国家利益、实现国家安全目标提供了路线图，标志着美国网络空间的目标与内容已经明确从美国自身扩展到全球。

把网络空间视为与陆、海、空、天并列的作战领域，通过有效组织、训练和装备，充分利用和挖掘网络空间的潜力。

运用新的防御行动理念，保护美国国防部的网络和系统。首先，采取“网络卫生”行动提高网络安全；其次，为阻止和减少内部威胁，将加强员工通信、员工问责、内部监控和信息管理能力；再次，将形成有效的网络主动防御能力，防止对美国国防部网络和系统的恶意入侵；最后，制定新的防御行动计划和计算架构。以上4步将共同形成适应性强的美国国防部网络和系统主动防御体系。

加强与其他政府部门和私营机构的合作，实现一体化政府网络空间安全战略。美国国防部将加强与其他政府部门的合作，同时，也将加强与国防工业基地的合作，其中包括提供防御技术、武器系统、政策与发展战略和人力资源的公共、私营机构和企业。

建立与美国盟国和国际伙伴之间的合作，加强网络空间安全。美国国防部用国际关系

来实现网络空间与国际伙伴的共同利益。这些努力体现在发展共享预警、增强能力建设和进行联合培训上。

建立一支卓越的网络行动队伍,提高信息技术创新能力,巩固美国在网络空间中的优势地位。美国国防部将整合美国的科学、学术和经济各方面资源,组织一批有才华的文职或军事人员在网络空间中开展行动。此外,美国国防部将遵循以下五个原则促进信息技术创新:第一,行动过程和法规必须符合技术发展的周期;第二,进行渐进式的测试,而不采用大规模、复杂的系统部署;第三,放弃或推迟一些专用项目,以实现快速的渐进式发展;第四,信息技术改进需求将根据美国国防部系统的关键程度而采取不同层次的处理;第五,提高安全性的措施将被应用于国家安全部购买的所有系统中。

报告中提出的五项倡议的具体内容可概括为:

一是确定应有地位。国防部将网络空间视为作战区域,对其实施组织、训练,并予以装备,以便国防部能全面利用网络空间的潜力。

二是进行主动防御。国防部将应用新的防御作战概念保护国防部的网络和系统。

三是关键设施防护。国防部将与美国其他政府和私营部门合作,共同实施政府范围内统一的网络安全战略,在保护军事网络安全的同时,加强重要基础设施的网络安全防护。

四是集体网络防护。国防部将与美国盟国和国际合作伙伴建立牢固的关系,以加强整体的网络安全。

五是加强技术创新。国防部将通过杰出的网络专业队伍和快速的技术创新,提升国家的创造力。

该《战略》是统筹美军网络空间领域发展的纲领性文件,旨在全面掌控网络空间主导权,谋求美国在网络空间的霸主地位。美国近年来在网络空间领域动作频繁,其扩大自身在网络空间总体优势的意图已显露无遗。

#### 4. 先发制人的网络控制战略

为了维持网络空间的绝对优势和不受挑战的全球领导地位,美国的网络空间战略总体上体现出先发制人的特点。该战略经历几届政府逐渐形成,其构建亦有一定步骤。第一是构建网络空间的敌人。第二是网络空间安全化。第三是制定相应政策和措施,国内层面包括组建网络战司令部、布置许多相关部门参与网络战的研究、在实践中试验各种网络武器、利用强大的技术力量施行全球网络布控等;国际层面包括主宰网络空间技术标准、把握着网络空间的控制权、加强网络空间联盟并发展伙伴关系等。

美国先发制人的网络空间战略对美国及国际社会都存在复杂的影响。从美国自身角度看,战略收益与风险参半。在国际层面上,美国先发制人的网络空间战略的影响有如下几点:第一,它将推动网络空间的军事化。网络空间军事化是指相关政府和军队发展网络攻击能力和赢得网络战能力的趋势。第二,美国先发制人的网络空间战略会引发网络军备竞赛,而这可能是目前为止对全球安全环境最广泛的破坏因素之一。第三,美国先发制人的网络空间战略增加了国家间在网络空间爆发冲突的风险。第四,美国先发制人的网络空间战略还必然影响网络空间行为规则的确立,从而破坏网络空间国际秩序。

### 2.1.3 美国网络空间的全球战略

可以说,美国对网络空间的重视程度前所未有,第一次把国际战略与网络政策相结合,将其与“二战”后建立经济和军事全球框架相提并论。从此,开始从政治、经济、安全和军事等领域全面规划网络空间发展和治理。

美国网络空间全球战略,是一个庞大的国家战略体系,涉及政治、外交、经济、军事、安全、情报、执法、技术等各个领域。美国希望,网络空间的未来发展是由美国与国际社会一起促进并建立开放、互动、安全、可靠的信息和通信基础设施,以此来支持国际贸易,加强国际安全,并促进言论自由和创新。为了实现这一目标,美国致力于建立和维护一种网络空间环境。同时,美国将努力维持伙伴关系,并全力支持遵守网络空间的法律法规。

遵循三项基本原则,即保护基本自由、隐私和信息自由流动。在基本自由方面,美国认为不能无视那些有邪恶意图的互联网用户,必须对网络空间的自由言论也要加以适当限制。在隐私方面,美国主张通过相应的调查机构进行执法,同时通过相应的司法审查和监督来保护个人权利,确保法律法规的一致性。在信息自由流动方面,美国认为,网络空间必须保持一个鼓励创新、创业的公平的竞争环境,而不是去任意破坏信息自由流动。

推出三大努力方向。为推进互联网的繁荣、安全和开放,美国将综合利用外交、防务和发展手段,并将这三个方面作为重点努力方向。外交方面,美国提出了创造激励机制,以便对开放、兼容、安全、可靠的网络空间的内在价值达成共识,并且建立起利益相关者共同工作的国际环境。国防方面,美国提出将同其他国家一道反对破坏网络和系统的行为,劝阻和制止恶意行为,并保留采取必要和适当措施的权利来保护这些重要的国家资产。发展方面,美国提出在国外将推动网络空间安全能力的建设,并在建设更为开放、兼容、安全、可靠的网络方面与合作伙伴建立更为密切的关系。

从总体上看,网络空间全球战略在操作层面突出强调两大核心理念,执行两大路线。一是强调保障国家安全,实施网络安全路线;二是强调主导国际政治,实施网络外交路线。两大路线既有不同侧重,又有相互交叉,分别由不同的国家部门具体负责。网络安全路线主要由美国国防部负责,比如美国网络司令部、国土安全部计算机应急响应小组等,研发网络战技术装备,发展新型网络战武器,承担防御网络攻击,保护国家安全等任务。网络外交主要由美国国务院负责,比如美国国务院及驻外使领馆、非政府组织国家民主基金会等,承担输出价值观念,影响国际政治的任务,在西亚、北非政局动荡风波中呼风唤雨。两条路线的基础就是,信息产业和技术由政府部门和私营部门共同推动发展。

战略的总体策略,就是凭借网络技术、设施、内容等优势,牢牢掌控网络空间的主导权和控制权,将网络优势转化为经济优势、政治优势、文化优势和军事优势。这在实际操作层面,根据不同路线,形成了不同策略。网络安全路线,强调用网络信息技术保障国家信息安全,形成了“网络空间安全策略”。美国前总统奥巴马连续发布了一系列文件,强调网络空间是关系美国安全的重要领域,提出先发制人的战略理念,以确保网络空间的绝对安全。网络外交路线强调按照美国全球利益主导国际政治关系,形成了“21世纪治国方

略”。美国前国务卿希拉里，就曾经提出基于“国家之上、国家之中、国家之下”理念的“21 世纪治国方略”，将网络外交视为 21 世纪美国外交战略的优先目标。

按照设想，美国将在全球着力推进七大重点计划，并在相关战略领域发挥领导作用。在经济领域加强接触，确保互联网为全球繁荣和科技创新做出贡献，并加大保护知识产权；在网络安全领域增进合作，增强美国及全球互联网的安全性、可靠性及灵活性；在执法领域加强网络立法和执行力度，提高全球打击网络犯罪的能力；在军事领域与盟友通力合作，提高盟友应对网络威胁的能力，并确保美国军用网络的安全；在互联网管理领域加强各国间的沟通交流，保障全球网络系统（包括域名系统）的稳定和安全；在国际发展方面援助合作伙伴构建“数字基础设施”，帮助提高抵御网络威胁的能力；在网络自由方面加强保护隐私，促进网络表达自由、集会自由及结社自由。此外，还强调与非国家行为体合作，明确提出政府要和公民社会合作，和各个国家公民社会合作，推动国际战略实施。

## 2.2 美国网络空间作战基本政策和策略的制定

从 1993 年 1 月克林顿上台执政以来，美国民主、共和两党政府和美军方推出了一系列国家层面的网络空间的战略性指导文件，特别是近年来颁布实施了各种战略计划和政策，涉及网络空间的计划和政策数量之多、种类之全、层次之细，远远领先于世界其他国家，充分展示了美国军政各界对网络空间“全局性”“基础性”“综合性”和“聚能性”的高度重视。

网络空间的发展大致经历了计算机网络空间、电磁与网络融合空间、泛在网络空间等三个阶段。从克林顿到小布什，再到奥巴马，美国国家网络空间战略经历了从被动防御到主动攻击的演化过程。从总体上看，可大致分为以下三个阶段：第一阶段是克林顿政府推行的国家信息基础设施的全面建设行动计划与重点防御战略的制定；第二阶段是小布什政府极力主张的攻防兼备，确保网络空间安全的国家战略的制定；第三阶段是奥巴马政府奉行先发制人战略，加强争夺网络空间霸权政策和策略的制定。

### 2.2.1 国家信息基础设施的全面建设行动计划与重点防御战略的制定

在克林顿时代，特别是在“9·11”事件发生之前，在没有发生重大网络信息安全事件的情况下，美国的网络空间战略的主题在于网络信息基础设施保护，重点在于“全面防御”，主要针对网络发展过程中出现的非战略意义上的网络安全问题，如网络犯罪、窃密等。

早在 1993 年 9 月，克林顿政府公布“国家信息基础设施（NII）行动计划”，即通

常所称的“信息高速公路计划”，将网络和信息的安全问题正式提升到“国家基础设施”的高度。

1994年9月，美国又提出建立“全球信息基础设施（GII）”的倡议，建议将各国的NII互联起来，组成世界范围的信息基础设施。从而推动美国互联网的快速发展。

1995年8月1日，美国陆军训练与条令司令部颁发了题为“信息战概念”的《525-69手册》，提出将所有维度（海、陆、空、天）的作战空间和战场系统（指挥控制系统、机动系统、火力支援系统）用数据链连接起来，建立态势感知共享加上具有连续作战能力的“21世纪部队”，使之能够比敌人更迅速、更精准地实施侦察、制定决策、展开行动。

1996年，美国专门制定并颁布了《电信法》和《国家信息基础设施保护法》，对有关计算机犯罪问题及对互联网关键基础设施的破坏做出了界定。

1998年5月，克林顿政府发布了第63号总统令（PDD63）：《克林顿政府对关键基础设施保护的政策》，再次将其提升至“关键基础设施”的高度，并首次提出了“信息安全”的概念和意义，并要求最迟于2003年建立一个可靠互联安全的信息基础设施，并形成相关保护能力。为此还设立了关键基础设施保障办公室，指定中央情报局、商务部、国防部、能源部、司法部、联邦调查局、交通部、财政部、联邦紧急事务处理局、国家安全局等拥有最为关键系统的政府部门作为第一批实施信息安全保护计划的关键部门。

1998年10月，美军发布了《信息作战联合条令》，称信息战就是影响敌方的信息和信息系统，并保护己方的信息和信息系统。……信息优势就是使用信息并阻止敌人使用信息的能力。

1998年年底，美国国家安全局制定了《信息保障技术框架》，提出了“深度防御战略”，确定了包括网络与基础设施防御、区域边界防御、计算环境防御和支撑性基础设施的深度防御目标。

1999年，美国正式实施“国家网络安全培训计划”，制订了包括建立“网络安全保障教育和学术交流中心”在内的“国家信息保障教育与培训规划”。1999年12月，克林顿政府首次在国家安全战略中正式运用“网络安全”这一概念，将之从信息安全中剥离出来。

2000年1月，美国政府制定了《信息系统保护国家计划》（NIPP1.0），对美国政府信息网络安全工作做出了较为全面的规划，提出了网络信息安全关系国家战略安全，将重要网络信息安全放在优先发展的位置，并强调对国家信息基础设施保护的概念，这意味着美国的互联网安全政策开始在美国的整体国家安全战略框架中获得了独立的位置。另外，将信息安全保护分为十项内容，涉及脆弱性评估、信息共享、事件响应、人才培养、隐私保护以及法律改革等；并列出了最有可能发起网络攻击的6大“敌人”：主权国家、经济竞争者、各种罪犯、黑客、恐怖主义者和内部人员。2000年12月发布的《全球时代的国家安全战略》誉为“首个国家网络安全战略”，这标志着美国政府将网络安全提升至国家安全战略层面予以高度重视。

综合来看，克林顿时期美国在网络空间的战略重点强调的是互联网关键基础设施保护的概念，并把重要信息系统的安全放在优先发展的位置，主要围绕“准备与预防”“侦察与反应”“建立坚实基础”三个目标来保护美国的网络空间安全。“准备与预防”就是采取

必要措施,使对美国关键信息网络进行重大、成功袭击的可能性最小化,同时建立强大的基础设施,确保网络受到攻击时维持网络的有效性;“侦察与反应”就是实时确认和评估网络袭击,然后牵制这种攻击,并迅速从袭击中恢复过来,重建受损的系统;“建立坚实基础”就是建立机构、教育民众、制定法律,做好“准备和预防”“侦察和反应”,以便更好地应对针对美国的主要信息网络的袭击。

在此阶段,由于中国互联网的发展和普及尚处于“蓄势待发”的初始阶段,互联网在中国社会经济政治等的影响和融合方面,力量总体不大,中国在网络空间还尚未出现可以对美霸权构成威胁的软硬件条件。因此,此时美国在对华网络空间的战略措施主要集中在防范针对来自中国零星黑客的攻击行为,以及利用互联网对华进行有害信息渗透和干扰。

### 2.2.2 攻防兼备,确保网络空间安全的国家战略的制定

2001年,“9·11”事件的发生,打破了美国本土“山巅之城”天然免疫的神话,改变了美国政府及国内民意对威胁来源与性质的判断,使其认识到对美国国家安全构成直接、紧迫威胁的并非像中国那样的“拥有可怕资源基础的军事对手”,反恐成为美国国家安全战略的首要任务和目标。在网络空间,大量恐怖分子以信息网络为媒介对美国日益依赖的网络基础设施发动频繁攻击,极大威胁着美国国家安全利益。“网络恐怖主义”已成为美国政府的心腹大患。

“9.11”事件以后,小布什政府以反恐、保障国家安全的强势姿态上台执政,严重关切以互联网为核心的关键基础设施的脆弱性的问题,高度重视网络攻击对国家安全带来的重大威胁。其先后发布了一系列强有力的政策、法令,将美国关键基础设施监测体系推入全面建设的轨道。

2001年10月,小布什政府发布行政命令《信息时代保护关键基础设施》,将克林顿时代的关键基础设施保障办公室全面升格为总统关键基础设施委员会,其成员包括国务卿、国防部部长、司法部部长、商务部部长、行政管理及预算局局长、科学与技术政策办公室主任、国家经济委员会主席、总统国家安全事务助理、总统国土安全助理等官员。同时签署《爱国者法案》,允许以反恐为目的对网络通信进行拦截。

2002年,美国通过了《政府信息安全改革法》,将政府信息安全工程划分为安全管理、安全技术实施和安全评估三大阶段。这一年,美国国防部向国会提交《网络中心战》(Network-Centric Warfare)报告,提出将网络中心战作为国防转型的指南。该报告称:“以网络为中心的部队是一支能够创造并利用信息优势,从而大幅度提高战斗力的部队,它能够提高国防部维护全球和平的能力,并在需要其担负恢复稳定的任务时在所有各种类型的军事行动中占据优势地位。”

2002年9月,美国“总统关键基础设施保护委员会”颁布了确保网络空间安全的国家战略——“网络安全战略”。该战略为确保网络安全提出了5个部分共86项劝告。在此基

础上，拟定了《美国的国家网络安全战略计划》，为美国关键信息技术（IT，Information Technology）基础架构提供综合性保护，在确保美国军民网络信息系统安全的情况下，攻击和破坏敌方的网络信息系统。

2003 年 2 月，小布什政府发表了《国家网络安全战略》报告，正式将网络安全提升至国家安全的战略高度，从国家战略全局对网络的正常运行进行谋划。同年 2 月中，又颁发了《关键基础设施和重要资产物理保护的的国家战略》。这份文件把通信、IT、国防工业基础等 18 个基础设施部门列为关键基础设施，把核电厂、政府设施等 5 大项界定为重要资产。同年 2 月 14 日，美国颁布了《确保网络空间安全国家战略》。该份文件长达 76 页，提出了保护关键性基础设施的目标和加强政府与私营部门合作的原则，分析了网络空间的构成及其重要地位，指出确保网络安全是美国国家安全战略的一个重要组成部分，为美国保护网络空间安全确立了指导性框架和优先目标。该文件确定了在网络安全方面的三项总体战略目标和五大重点任务，还提出该战略实施过程中应遵循的六条指导原则。

2004 年，美国在参谋长联席会议制定的《军事战略报告》中提出要发展在“全球公域”——包括太空、网络空间、国际水域和空域的行动能力，这是国防战略八项变革的焦点之一。该战略首次把网络空间与陆、海、空、天四个传统战争领域相提并论，成为第五个美国重点争取的军事竞争领域，并在报告内声明这五个领域内的其中之一遭到攻击时，美国可以在另一领域内进行还击。

2005 年 1 月，美国国防部发布了“国防部网络防御”备忘录，提出了改进国防部计算机安全的具体要求，要求把保护国防部计算机网络系统放在一切工作的首位，为实现美军《2020 联合构想》中提出的信息网络作战提供了有力保障，标志着美军“以进攻为主”向“信息进攻和信息防御并重”的信息战方针的重大转变。

2005 年 2 月，美国总统 IT 咨询委员会向总统小布什提交《网络空间安全：迫在眉睫的危机》的紧急报告，对美国 2003 年的网络安全战略提出了不同看法，并提出十二项共 25 条建议。2005 年 3 月，美国国防部公布的《国防战略报告》，更明确地将网络空间与陆、海、空和天定义为同等重要的、需要美国维持决定性优势的五大空间。

2006 年 4 月，信息安全研究委员会发布了《联邦网络空间安全及信息保护研究与发展计划（CSIA）》，确定 14 个技术优先研究领域，13 个重要投入领域。

2006 年 6 月 30 日，小布什政府发布了《国家基础设施保护预案》。这一年美国国防部还秘密发布了《网络空间作战国家战略》。空军颁布《空军战略计划》，明确把网络空间正式界定为一个全新作战领域，提出了掌握天空、太空和“网络空军”控制权的概念。值得特别指出的是，在小布什政府执政的中后期，美国军方的网络空间安全战略逐渐发生了重大转变，由早期的防御为主转变为攻防兼备。例如，在软杀伤网络空间作战武器方面，美军研制出 2000 多种计算机病毒武器，如蠕虫、木马和逻辑炸弹等。在硬杀伤网络空间作战武器方面，美军研发出电磁脉冲弹、次声波武器、激光反卫星武器等，可对别国网络的物理载体实施攻击。

2006 年 12 月，美国参谋长联席会议联合国防部制定了《网络空间作战国家军事战略》。该文件完整界定了网络空间领域，分析了在此领域的威胁和薄弱环节，并对未来态势进行



了客观分析。其中,最为重要的内容是确立了网络空间的军事战略框架,包括美军在网络空间的军事战略目标,以及实现这一目标的方式和方法:战略目标是确保美国在网络空间的军事优势;实现方式分为五个基本方式(信息作战、网络作战、动能攻击、法律强制和反情报,以及主题和信息管理)和六个使能方式(科技、合作、作战情报数据支持、态势感知、法律政策和人力)。同时,提出要在四个方面加强建设:一是在竞争对手决策周期里获取和维持主动行动优势,二是利用网络空间使整个军事行动领域进一步整合军事能力,三是建设网络行动能力,四是管理网络空间行动的风险。这些是确保在网络空间获取军事优势的全面战略。

2008年1月8日,小布什总统签署和推出一项预算高达300亿美元的《国家网络安全综合计划》(CNCI, Comprehensive National Cybersecurity Initiative),也被称为“网络空间的曼哈顿计划”,涉及反情报、供应链安全、预防入侵、技术研发及威慑战略等。该计划囊括了“推行‘可信互联网连接’计划,缩减外部接入点的数量”“在联邦企业广泛部署‘爱因斯坦2’与‘爱因斯坦3’”“构建信息共享体系以提升整体态势感知能力”“保护公民隐私与自由”“扩大网络安全方面的知识 with 技能教育”“开发全球供应链”“确定联邦政府在关键基础设施保护工作中的职责”及“明确计算机应急响应小组的任务”8项主要内容。小布什赋予国防部更大的网络空间作战反制权,允许美军主动发起网络攻击,要求美军具备进入任何远距离公开或封闭的计算机网络的能力,然后潜伏在那里,保持“完全隐蔽”,并“悄悄窃取信息”,防止美国遭受敌方的电子攻击,并能对敌方展开在线攻击。保卫美国网络空间的国家战略是一项综合性的战略。其中阐述了三个战略重点:一是防止针对美国关键设施的网络攻击;二是提升应对网络攻击的抗毁性;三是使网络攻击的破坏降至最低,并缩短恢复周期。

美国政府在国会和公众的压力下,于2008年下半年还是公开了CNCI的12项重大活动的基本信息:(1)通过可信因特网连接把联邦的企业级规模的网络作为一个单一的网络组织进行管理;(2)部署一个由遍布整个联邦的感应器组成的入侵检测系统;(3)寻求在整个联邦范围内部署入侵防御系统;(4)对研发工作进行协调并重新定向;(5)把当前的各网络行动中心相互连接起来,加强态势感知;(6)制订和实施一个覆盖整个政府部门的网络情报对抗计划;(7)增强涉密网络的安全;(8)扩大网络安全教育;(9)定义和制订能“超越未来”的持久的技术、战略与规划;(10)定义和发展持久的遏制战略与项目;(11)建立全方位的方法来实施全球供应链风险管理;(12)明确联邦的角色,将网络安全延伸到关键基础设施领域。其中共有四个战略要点:一是在对手的决策周期内,获取并保持作战的主动权;二是整合整个军事行动中的网络空间能力;三是建立起网络空间作战能力;四是控制网络空间作战行动的风险。

2008年10月,美国空军正式启动出台了《空军网络司令部战略规划》,提出了空军开展网络空间作战的构想。2008年12月发布了约翰·G·格鲁姆斯为美国国防部领导层所写的美国国防部《网络作战战略构想》。目的是传达国防部首席信息官向新的网络作战功能转移的构想和长远目标。它为国防部的合作伙伴以及参与全球信息栅格行动和防卫的其他机构提供了参考和借鉴。提出了“作战人员、日常工作人员以及情报用户和决策者完全

利用全球信息栅格的能力，把网络作战的威力转变为一支部队力量的倍增器”的战略构想。执行这一战略构想的下一步发展计划是，需要国防部各级部门制定、实施网络作战计划，以解决计划、界定、资金、采购以及操作网络作战功能的相关问题。建立政策、架构、实施策略以及部署时间表，以满足为每个增量确定的具体功能。

另外，这一时期发布的其他重要文件还包括：2000 年签署的《国土安全法》；2003 年发布的《联邦信息安全管理法》《关键基础设施和重要资产物理保护的国家战略》；2008 年美国战略与国际研究中心向白宫提交了《保护网络空间安全》的报告；2009 年年初发布《海军网络司令部战略规划》；2009 年发布了《美国空军网络空间的发展蓝图》。

可以说，对恐怖主义及其支持国进行网络安全防范，并对其推行先发制人的针对性打击，是小布什政府时期美国网络安全工作的核心任务。与克林顿时期主要集中于保护本国的关键基础设施及重要系统的战略重点相比，小布什政府的网络空间战略总体上呈现出的是进攻性的特质，这一点也可从美国网络空间安全在整体国家安全中的地位及优先位置的变化情况得以佐证。总体而言，小布什时期美国在网络空间战略的主题主要为“网络反恐”，重点在于基于实力的威慑以及“网络攻防结合”。

### 2.2.3 先发制人，加强争夺网络空间霸权的政策和策略的制定

2008 年，席卷全球的金融海啸，以及美国在伊拉克、阿富汗反恐战争的久拖不决的情况下，美国民众反恐情绪的淡化态势已不够支撑以先发制人、单边主义为主要性质和特征的美国网络空间安全战略。以改变和转型为标签的奥巴马政府也日趋明晰了美国在网络空间的战略目标，即通过对网络空间秩序的塑造来保持自身的战略优势，在其入主白宫伊始，美国就高调突出网络空间安全战略。例如，在 2009 年 2 月美国政府宣布将网络安全作为维护美国国家安全的首要任务之一，并就此要求有关部门对美国的网络安全状况展开为期 60 天的全面评估，以检查联邦政府部门保护机密信息和数据的措施。具体来看，奥巴马政府主要从基础设施保护、管理运行机制、网络军事发展、外交国际等方面入手，出台了一系列组合拳，强力维护美国在网络空间的霸主地位。在此期间美国发布的网络空间重要战略包括以下一些方面：

2009 年 1 月，奥巴马出任美国总统后不久，便根据美国战略与国际问题研究中心提交的《确保新总统任内网络电磁空间安全》专题报告，提出要像 1957 年 10 月苏联发射第一颗人造地球卫星那样，举行类似的全民大讨论，提高美国民众网络电磁空间安全意识。

2009 年 3 月，服务于国会两院的政府责任办公室发表《国家网络安全战略》报告，根据国土安全部在过去七年的表现，呼吁从加强网络分析和预警能力、加强在网络演习中完成行动的能力、改进基础设施控制系统、提高国土安全部在网络破坏中的恢复能力、处理网络犯罪五个方面着手解决网络安全问题。6 月，总统行政办公室发布《网络空间政策评论》报告。

2009年3月,奥巴马政府针对小布什时期提出的国家网络安全综合倡议进行了评估,发布了《国家网络综合安全倡议:法律授权和政策考虑》的评估报告,该报告详细分析了信息化时代网络空间作战的法律与政策问题,认为美国政府要高度关注针对网络信息关键基础设施的攻击,提升针对这些设施的防御能力。“保护国防部太空和网络空间等设施在内的关键基础设施,增强其大规模杀伤性武器、太空和网络空间的攻击能力,使侵略者必须对其行为负责,并使其无法做到在新领域内发现美国目标或使用新代理人攻击目标。”

2009年3月11日,美国政府责任局发布《美国国家网络安全战略:需要进行的改进》报告,指出应进一步加强的关键网络安全领域,并就完善国家网络安全战略提出了十几条建议。同时,加强了网络电磁空间安全立法和宏观规划。

2009年3—4月间,美国国会先后提出了《2009网络空间安全法案》(773号)和《国家网络电磁空间安全顾问办公室法案》(778号)。上述法案赋予总统和商业部等相关部门广泛权力,包括审查认证网络安全工作人员、必要时关闭网络等。值得注意的是,奥巴马政府在大幅削减导弹防御系统、F—22战机采购费用的同时,加大了对网络安全的投入,加速推进网络战部队建设。这一系列做法体现了奥巴马政府网络电磁空间战略的思路,即从实体战场逐步转向网络,达到从“实体消灭”到“实体瘫痪”的目标。

2009年5月29日,奥巴马公布了《网络空间政策评估——保障可信和强健的信息和通信基础设施》的报告。他在演讲中强调,“美国21世纪的经济繁荣将依赖于网络空间安全”,称“网络空间安全威胁是对我们举国面临的最严重的国家经济和国家安全挑战之一”,并宣布“从现在起,我们的数字基础设施将被视为国家战略资产。保护这一基础设施将成为国家安全的优先事项”。该报告通过对当时美国网络安全政策和组织结构进行评估,提出美国必须向全世界表明将通过强有力的领导和对远景的规划严肃认真地迎接网络安全挑战。另外,还公开了新的联邦政府网络安全计划的轮廓。这标志着奥巴马政府已经把网络安全视为国家安全优先考虑的问题。奥巴马采取了两大重要决策:削减包括F—22战机在内的传统武器;高调组建网络司令部,大幅增加网络武器投入。奥巴马的网络空间作战战略显现出“攻击为主,网络威慑”的主题。

2010年1月,美国国防部发表《四年任务使命评估报告》,指出“网络中心战”应该被列为美军的“核心能力”,打造一支更加专业化的网络作战部队。2010年2月22日,美国陆军发布了《2016—2018年网络行动概念能力规划》。该文件首次由军方公开,较系统、详细地对网络空间行动的概念进行认识与理解,以及能力目标和理论进行了阐述。

2010年5月27日,奥巴马政府发布了《2010年国家网络安全战略报告》。该报告有一节专门阐述“保障网络空间安全”。2010年9月,《华盛顿邮报》披露,五角大楼力求在网络战争中先发制人,并达到“5D效果”(欺骗、拒止、分离、降级、毁坏5个英文单词首字母均为D)。

2010年7月,美空军率先颁布了《空军网络空间作战条令(AFDD3-12)》。该条令明确了网络空间作战部队的指挥控制关系、职责、作战实施方法,并详细描述了空军网络战的设计、计划、实施和评估流程。

2011年4月,白宫发表《网络空间可信身份国家战略》,从构成美国主导的身份标识

生态系统和推行美国主导的网络空间国际新秩序两方面，为美军做了技术定位，为制定网上行为准则和执法做了铺垫。2011年5月16日，美国白宫网络安全协调官施密特(Howard A. Schmidt)发布了美国政府出台的《网络空间国际战略》。该战略提出网络空间发展与防护的原则，确定了网络空间的行为规范，明确了美国政府的重点工作领域和应发挥的作用，高调宣布“网络攻击就是战争”，表示如果网络攻击威胁到美国国家安全，将不惜动用军事力量。该战略还宣称要建造一个“开放、互通、安全和可靠”的网络空间。报告勾勒出了实现政策路线图，基本涵盖了“美国所追求的目标”，并列出了7项重点政策，被称为美国在21世纪的“历史性战略”。6月4日，国防部长盖茨在新加坡发表演讲时，首次表明在确认遭到来自他国的网络攻击时将“视之为战争行为并予以武力还击”。

2011年7月14日，美军主管网络安全事务的国防部副部长威廉·林恩正式公布了《国防部网络空间作战战略》(Department of Defense Strategy for Operating in Cyberspace)。该战略共40页，其中公布的非密部分13页，包括简介、战略背景、五大战略倡议三个部分，主要介绍了美军在网络空间领域的战略计划，指出了国防部的网络空间优势，对网络空间的威胁进行了分析判断，构筑网络战略体系，充分利用资源优势，实现主导网络安全体系，扩大网络空间作战范围，以确保网络空间整体优势，提高国防部和国防承包商网络系统的防御能力，从而谋求网络空间霸权地位。2011年11月还出台了《国防部网络空间政策报告》。

2011年11月，美国空军发布了《空军准则文件3-12：网络空间行动》。该文件系统地从空军的角度对网络空间的作战环境、面临挑战、作战原则、指挥与组织关系以及规划、执行和评估等问题进行了阐述。该准则文件还描述了网络空间域与其他几个传统作战域的交叉关系。

2012年4月，美国联合参谋部发布了联合出版物《JP6-01 联合电磁频谱管理作战》。该文件系统地阐述了与联合电磁频谱管理作战相关的业务概述、行动规划、指挥协调关系和原则等，并将网络空间及网络部队的相关问题纳入其中。

2012年7月6日，奥巴马签署了关于《分配国家安全和应急准备通信功能》的行政命令，绕过国会的反对，获得了必要时在互联网上宣布进入紧急状态并关闭互联网的权力。

2012年7月11日，美军还出台了《国防部云计算战略》。从表面上看，该战略计划是为了在全球及美国经济不景气的大环境下进一步优化美军信息化建设资源的“明智选择”，但从更深的层面来分析，这一计划其实代表着网络空间动态化、虚拟化、智能化，以及情报收集细粒化、分散化，信息处理与分发定制化、便捷化，并最终导致作战效能集中化的未来发展趋势。我们可以想象，随着各种攻防一体、飘忽不定、军民兼用的“网络战斗云”的出现，未来的网络战场建设必将出现全新的景象。

2012年8月，美国空军发布了“X计划”技术方案演示计划——《网络空间对抗能力技术方案演示验证计划(修订版)》。该方案重点围绕网络空间攻击、网络空间防御、网络空间攻击能力发展、不接入网络条件的网络对抗能力发展与评估、网络空间态势感知能力、可视化评估能力、基于效果的能力发展、差异化的网络空间对抗技术与能力共8个方面开展技术方案演示验证。

2012年9月,美军公布《美军联合作战顶层概念:联合部队2020》,提出了全球集成作战的概念。

2012年11月,美国联合参谋部发布了联合出版物《JP3-13 信息作战》。该文件系统阐述了与信息作战相关的信息化环境、信息作战单元、作战规划、集成、联合以及跨国信息作战等问题,其中考虑了网络空间行动的因素,描述了与电子战之间的关系。同月,美国陆军司令部发布了《FM3-36 电子战》。该文件提供了陆军准则的电子战策划、筹备、执行和评估,以支持统一的陆地电子战行动。本月,在总统批准了新战略、国防部调整了21世纪国防优先次序的背景下,美国海军发布了《海军网络能力2020》指南。该指南强调了网络空间行动对美国联合部队取得成功的重要性,描述了实现海军网络空间作战的构想以及海军主要的战略举措,并介绍了主要的最终状态。

2013年,奥巴马第二任期刚刚开始,便签署了加强网络安全的行政命令,网络安全成为首推议题。2月5日,美国参谋长联席会议以内部文件的形式发布《JP3-12 网络空间作战令》。该条令以“国家军事战略网络战实施计划”为基础,对网络空间作战概念进行了重新修订,强调网络空间军事行动的独特性,从顶层设计上统一美军网络空间联合作战概念、机构职责、联合程序和方法,进一步规范了网络战的指挥控制和相互关系。2月12日在国情咨文中,奥巴马要求议会加强立法,重视网络安全。3月12日,美国16家情报机构发布了《美国情报界世界范围威胁评估》年度报告,强调“计算机网络的数字攻击已经取代了其他的安全担忧”。美国国家情报总监克拉珀也将其列为“头号安全威胁”,这在2001年“9·11”事件之后尚属首次。

2014年2月,美国陆军发布了野战条令《FM3-38 网络电磁作战》,明确了网络空间的作战因素和约束条件,为陆军规划、集成与协调网络电磁作战提供了总体原则、策略和流程。该条令确定了作战指挥官在网络电磁作战中的核心地位,明确由作战指挥官负责将网络电磁行动集成并协调到所有指挥层次和作战任务领域,同时由电子战参谋、频谱管理员、情报员、火力保障员、民事行动参谋、空间支援小组和军法总署成员组成网络电磁行动小组,负责为指挥官提供制定决策所需的信息。该条令还明确了网络战的三种重要行动(计算机网络战、电子战和电磁频谱管理)的规划方式和实施流程,阐述了陆军在作战行动中如何开展各项网络战,以及陆军在联合网络战中需要考虑的问题。

2014年3月4日,美国国防部发布了2014版《四年防务评估报告》,列举了美国防务战略日程的优先事项:推进亚太再平衡;维护欧洲和中东地区的安全与稳定;在全球范围内(重点是中东和非洲)打击暴力极端分子和恐怖主义;在美国军事力量总体“瘦身”的情况下保护美国对技术的关键投入;努力构建新型伙伴关系,强化关键的同盟和伙伴关系。提出将网络作战能力上升为最重要的作战力量。

2014年10月21日,美军在网上对外公开了其首部《网络空间作战》联合条令。美军作战理论由作战构想、作战概念和作战条令三部分构成,指导美军作战和训练的作战条令是核心。美军作战条令分联合作战条令和军种作战条令,分别用于指导其联合和军种的作战训练。《网络空间作战》联合条令处于联合作战条令序列的战术层级,规定了网络空间作战联合的战术、技术和操作程序,在整个军事行动范围内如何规划、准备、执行和评估

网络空间联合作战，可为联合部队指挥官、参谋人员，以及相关下级指挥官组织网络空间作战提供指导和帮助，也是指导美军组织和实施网络空间作战与训练的权威性文件。

2015年2月13日，奥巴马签署《促进私营部门网络安全信息共享》的行政命令。其主要内容是建立一个私营部门之间信息共享并且与政府信息共享的框架。通过发展“信息共享和分析组织”，使其在政府和私营部门之间充当信息共享的平台，对私营部门向政府透露企业隐私引起的不适感起到缓冲作用，对政府获取企业数据起到监督作用。

2015年4月1日，奥巴马签署了三年内的第四个关于网络安全的行政命令，题为《封锁参与通过网络进行的重大恶意活动的特定个人资产》。这一行政命令打击对象为来自国外的网络黑客，针对危害“国家安全、外交政策、经济稳定”的严重威胁，采取的措施包括冻结资产、禁止与美国人的生意往来、禁止入境和禁止获取美国货物或技术。

2015年4月23日，美国发表《国防部网络战略》。国防部部长卡特通过在斯坦福大学的演讲向公众对战略构想进行宣传。这份新版的网络战略对2011年美国出台的《国防部网络空间作战战略》进行了全面修订，明确了网络威慑的关键地位，关键是网络威慑和防御，但是不排除采用网络攻击手段，强调建设和训练网络任务部队。其主要有以下新变化：

一是为提升网络力量建设重要地位提供新的依据。该报告进一步把美国在网络空间的威胁上升为“第一层级”的威胁。同时，该报告还将中国、俄罗斯、伊朗、朝鲜视为美国潜在的“网络对手”，这是其对网络威胁形势做出的最新、最严峻的判断。

二是为加快网络空间作战力量建设提供新的指导。报告重点明确了国防部在网络空间的三大任务和五大目标，并进一步细化133支网络战分队的建设目标。

三是为维持全面的军事优势打造新的支柱。报告明确提出，当美国面临针对美国本土或美国在网络空间利益的攻击时，美军可以进行网络作战，实施网络攻击。这是此次网络空间战略最重要的调整。未来，美军将把网络攻击作为重要的作战手段使用。这是美国在网络空间“动网就动武”理念的主要体现。

四是为重塑国际网络体系创造新条件。报告强调，对内重点加强军民协同，对外重点发展与盟友合作。合作的主要目标是分担成本和风险，推行对美国有利的国际行为准则，抢夺网络空间规则制定的话语权和主导权。

2015年7月，美国国防部先进研究项目局（DARPA）发布新版发展战略报告——《服务于国家安全的突破性技术》，阐明了在技术扩散加快的背景下，美继续维持当前的全球战略优势地位所面临的机遇与挑战。报告提出了四项主要战略投资领域及相关投资重点，其中DARPA提出利用大数据工具对大规模数据集进行分析，提高关键决策系统及其数据的自动化网络电磁防御能力。

2016年2月9日，奥巴马公布《网络安全国家行动计划》，将从提升网络基础设施水平、加强专业人才培养、增进与企业的合作等五个方面入手，全面提高美国在数字空间的安全。该行动计划中的多项决策值得关注，包括提议在国会2017财政年度预算中拿出190亿美元用于加强网络安全，第一次设立联邦首席信息安全官（CISO），下令成立国家网络安全促进委员会、联邦政府隐私委员会等。

另外美国陆军训练与条令司令部在2010—2014年相继发布了《美国陆军网络空间作

战能力概念计划（2016—2028）》《网络/电磁能力基础评估》和《美国陆军“陆地网络”白皮书（2018—2030）》，明确了美国陆军网络空间作战能力建设方向和路径，对网络空间作战能力发展进行了远景构想和长期规划。

总体上说，20世纪90年代以来，美国三位总统克林顿、小布什和奥巴马都将网络安全地位的提升作为一项基本政策。克林顿时期信息网络安全的主题是“关键基础设施”和“开创”；小布什时期信息网络安全的主题是“网络恐怖”；奥巴马时期信息网络安全主题“战略资产”。克林顿时期美国的信息安全主题以防护为主，重点在于“全面防御”，保障信息安全的主要手段还是以信息安全产品为主。小布什政府一方面继承了克林顿政府网络保护的特点，同时又强化了网络反恐的主题，体现攻防结合的特点。到了奥巴马政府增加网络攻击武器的投入，并筹建网军司令部，其网络安全战略已表现出“攻击为主，网络威慑”的特点。在奥巴马时期，美国单边主义、先发制人的网络空间进攻思维，以及实施的以积极防御为核心的网络威慑战略发挥到淋漓尽致的程度。美国的国家信息安全战略经历了一个“从被动预防”到“网络威慑”，从“适度安全”到“先发制人”的演化过程。

## 2.3 美国网络空间作战力量及其指挥控制机制

### 2.3.1 美国国家层面上的网络安全机构

美国网络安全组织架构的最高层是总统，也就是说，总统就是网络安全组织架构的设计者和责任人，主要通过出台战略、计划、总统令和行政令等政策文件，调整和完善网络安全组织架构；其次是政策执行机构，包括协调部门、政府部门、情报部门、军事部门，这些机构通过执行各自的职能，将维护网络安全的政策落到实处。

#### 1. 协调部门

克林顿总统时期在国家安全委员会中设立“安全、反恐与基础设施防护协调官”，向总统安全事务助理负责，同时成立“关键基础设施协调小组”，由所有涉及国家安全的政府部门组成，负责网络安全战略、政策的制定。小布什总统上台初期基本上沿袭了这种体制，但是“9·11”事件发生后，宣布成立新的机构——“总统关键基础设施保护委员会”，委员会主任直接向总统负责，该委员会直到国土安全部建立和运转后才被取消。奥巴马上任后不久，宣布成立“白宫网络安全办公室”，由该办公室负责协调美国联邦政府军事和民事部门的网络安全政策和行动，并向国家安全委员会和国家经济委员会汇报工作。同时，为了使信息技术和网络更有效地服务于美国外交政策，时任国务卿希拉里建立了“网络问

题协调办公室”，负责统一协调国务院各机构处理网络问题，协调国务院在网络问题方面的全球外交活动，就网络问题向国务卿提出建议。2009年年底，美国还成立了“全国通信与网络安全控制联合协调中心”，其主要工作就是协调和整合网络安全专职机构，以提高跨领域的保护网络空间安全的能力。

## 2. 政府部门

美国国内负责网络安全事务的联邦政府部门主要有：一是国务院，主要负责美国网络安全国际合作和网络外交工作。二是国土安全部，负责保护美国关键基础设施安全，并跨地区、跨部门协调网络安全应急事件管理；属下的国家网络安全局负责制定国家的整体网络安全战略及其总体规划。三是联邦调查局，主要负责打击网络犯罪和进行相关执法活动。四是商务部，主管网络安全相关标准的研究制定。五是国家保密局设立的计算机安全中心和网络攻击中心，负责网络空间的战略情报预警、网络攻防技术开发和网络信息战指导。为应对安全威胁，美国政府建立了六个维护网络安全的专职机构，即隶属国土安全部的“美国计算机应急响应小组”，隶属国防部的“联合作战部队全球网络行动中心”和“国防网络犯罪中心”，隶属联邦调查局的“国家网络调查联合任务小组”，隶属国家情报总监办公室的“情报界网络事故响应中心”，隶属国家安全局的“网络空间安全威胁行动中心”。其中，历经最多调整的部门是国土安全部，该部门是小布什政府2002年在20多个联邦政府机构合并的基础上组建起来的，其所属的信息分析与基础设施保护局负责关键基础设施保护工作，由国家基础设施保护中心（原属联邦调查局）、国家通信系统局（原属国防部）、关键基础设施保护办公室（原属商务部）、计算机安全分会（原属国家标准与技术协会）、国家基础设施建模与分析中心（原属能源部）、联邦计算机事故反应中心（原属总务管理局）等部门整合而成。具体职责包括：制定保障美国重要资源和关键基础设施的综合性国家计划；针对以关键信息系统为目标的攻击行为提供应急响应；在关键信息系统失效的情况下为私营部门和其他政府机构提供技术援助等。另外，美国联邦政府部门下设许多支撑机构和技术力量，也协助这些部门及机构开展网络安全工作。

2015年2月25日，美国总统奥巴马下令成立一个新的网络安全机构，名为“网络威胁情报整合中心”，旨在协调整合美国现有机构搜集的网络情报，加强美国应对网络威胁的能力。该中心侧重于把针对美国的外国网络威胁和影响美国国家利益的网络事件等有关情况“串联”起来，为决策者提供基于各个来源的分析报告，并为现有的网络安全机构（如全国通信与网络安全控制联合协调中心、全国网络调查联合工作组及网络司令部）的工作提供支持。2016年2月9日，奥巴马公布《网络安全国家行动计划》，提议在国会2017财政年度预算中拿出190亿美元用于加强网络安全，第一次设立联邦首席信息安全官（CISO），下令成立国家网络安全促进委员会、联邦政府隐私委员会等。“国家网络安全促进委员会”成员既包括政府外的战略、企业和技术专家，也包括议会任命的两党议员。委员会的任务是制定未来十年的详细行动建议和行动的路线图，包括提高网络安全意识，增强私有领域和政府部门的保护，保护隐私，维护公共安全以及经济、国家安全，使美国更



好地掌控数字时代的安全。

### 3. 情报部门

美国情报机构共有 16 个, 其中, 中央情报局是独立机构; 国防部下属 8 个机构, 分别是国防情报局、国家安全局、国家地理空间情报局、国家侦察局、空军情报监视侦察局、陆军情报与安全司令部、陆战队情报处和海军情报处; 国土安全部下属 2 个机构, 分别是情报与分析办公室和海岸防卫队调查处; 司法部也有 2 个下属机构, 即联邦调查局和缉毒局; 其他如能源部、国务院和财政部各下属 1 个机构。从 2013 年 8 月份斯诺登爆料的“黑色预算”文件中可以得知, 各情报部门的预算主要用于四項工作, 即管理与支援、数据收集、数据处理与开发, 以及数据分析。由于数据收集、处理和分析越来越多地依赖计算机网络, 因此美情报部门一方面格外关注通过网络获取情报, 另一方面极力防范网络间谍渗透, 网络安全成为情报部门近年来高度关注的领域。而且, 奥巴马上任不久便发布了《国家情报战略(2009)》, 要求保密、反间谍工作重点关注四大领域, 网络安全便是其中之一。由此, 网络安全在情报工作中的地位被提升至一个前所未有的新高度。

## 2.3.2 美军指挥控制链

美国于 1986 年颁布的《戈德华特—尼克尔斯法案》(又称《国防部改组法》)是对现行美军指控关系影响意义最大的法案, 该法案调整了美军在“二战”后实行的各军种独立指挥链模式, 正式确定了总统、国防部部长到作战司令官的作战指挥链, 从而奠定了美军“军令”“军政”分离的指控模式。

根据美军联合条令(JP)的定义, 美军现行的指控链主要通过“军令”“军政”两条主线来实施。其中, “军令”解决作战力量的“使用权”问题, 主要包括作战指挥(COCOM, Combatant Command)、作战控制(OPCON, Operational Control)、战术控制(TACON, Tactical Control), 分别从战略、战役、战术层面施行作战指控。“军政”解决作战力量“所有权”问题, 主要指行政控制(ADCON, Administrative Control)。

图 2-1 为美军指挥控制关系的简化模型图。由图可见, 美军的指挥控制链通过总统与国防部部长, 向下贯穿各级作战司令官。其中, COCOM 一般由总统或国防部部长赋予统一作战司令部司令官, 即地理作战司令官(GCC, Geographic Combatant Commander)与职能作战司令官(FCC, Functional Combatant Commander); OPCON 可由各级作战司令官行使, 其主要职能包括组织和部署作战力量、制定作战目标、分配作战任务等; TACON 一般由低级别的作战部队行使, 其职能主要包括对完成指定的使命或任务进行细致的指导和控制。美军的 ADCON 一般由各军种行使, 其主要职能包括部队编制、装备人员训练、后勤保障、人事管理等。

美军认为指挥控制是所有军事行动的核心, 其各级作战司令部的指挥控制体系历经多

年考验，已臻完善。但随着网络空间概念的兴起，各级相关作战力量的组建，特别是 2008 年《统一指挥计划》的颁布，在一定程度上影响了美军现行的指控关系。近年来，美军对网络空间指控关系的讨论一直没有停息过，而其争论的焦点就是各部门在网络空间作战中应该扮演什么样的角色。

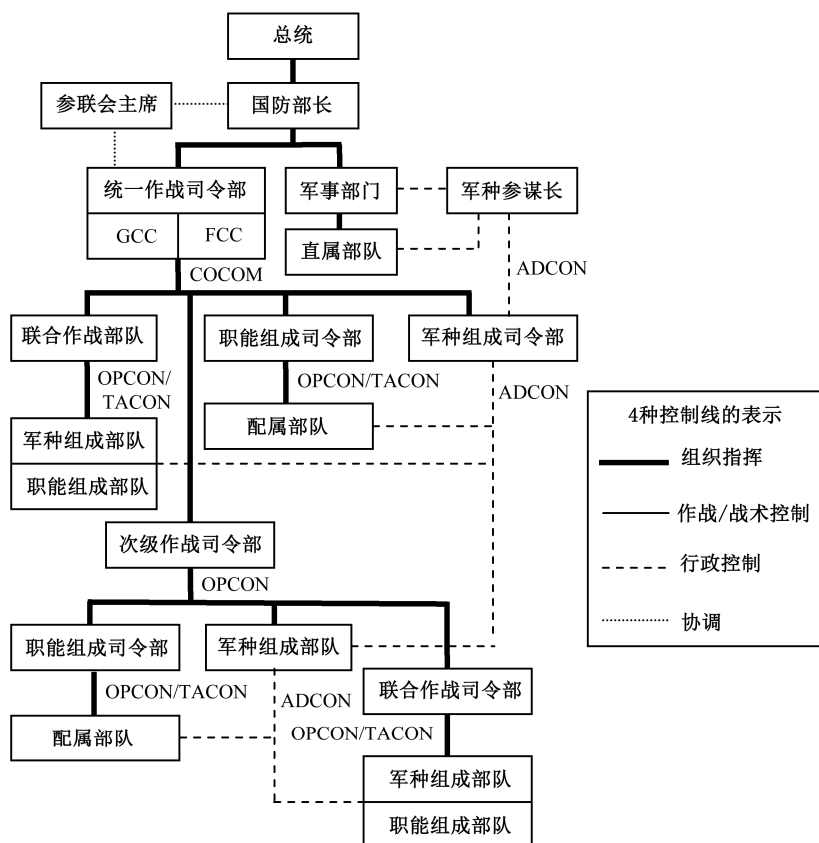


图 2-1 美军指挥控制关系的简化模型图

### 2.3.3 国防部组建的网络空间作战指挥机构及其职能

美国是最早建立网络空间作战部队的国家，也是最早将网络空间作战用于战争实践的国家。美国国防部 1995 年就开始组织“网络黑客”在网络空间开展全面信息对抗。1995 年 6 月，美军 16 名“第一代网络战士”从美国国防大学毕业。

1998 年 10 月，美国国防部批准成立“计算机网络防御联合特种部队”，主要负责保护五角大楼在美国本土和全球范围内的网络系统，应对那些对美军网络的攻击。

2002 年，美国总统小布什签署“国家安全第 16 号总统令”，决定组建世界上第一支网络“黑客”部队——“网络空间作战联合职能司令部”，也称“140 部队”，并于 2005 年 1

月正式运作，主要职责是对敌发动网络攻击，试验各种现有网络武器的效果，制定美国使用网络武器的详细条例以及培训网上攻击队伍。一旦爆发战争，将承担监控、摧毁敌网络系统以及窃取情报的任务。成员掌握着世界上最先进的网络技术，能够轻松渗入敌国军事信息网络系统，可以给系统注入病毒或摧毁系统。

2004年3月，美国国防部宣布成立网络进攻支援委员会，以提高军队网络进攻的能力。2006年年底，美国国防部组建了一支全新的部队——“网络媒体战部队”。其成员既是计算机高手，又是出色的“记者”，他们全天候24小时监控互联网，以便及时纠正错误信息，帮助美军对付“不准确信息”，并积极引导有利报道的传播。2012年，美国国防部组建美军北方司令部联合网络中心（JCC）。JCC主要负责3项任务：提高网络疆域的态势感知；提高司令部网络防御水平；应民事部门要求，向网络重要事故提供响应和恢复支持。

2009年6月23日，美国总统奥巴马授权国防部长盖茨正式签署了一份备忘录，宣布合并“计算机网络防御联合特种部队”和“网络空间作战联合职能司令部”这两支部队，组建美国网络司令部。该司令部已于2010年5月21日正式运行，位于国家安全局所在的马里兰州米德堡（Fort Meade），拥有千余名信息战专家，对目前分散在美国各军种中的网络空间作战指挥机构进行整合，统一指挥美国海、陆、空三军网络空间作战行动。这个新机构隶属于美军战略司令部的次级司令部，美国国家安全局长基思·亚历山大被提名为第一任司令。

美军战略司令部总部位于内布拉斯加州奥法特空军基地，于2002年由美国航天司令部和战略司令部合并而成，旨在将空间、信息对抗和进攻打击能力有机结合在一起，执行空间和全球打击，负责制定网络空间作战规划等任务。其任务领域为：网络战，导弹防御，空间和全球打击，情报、监视和侦察，以及大规模杀伤性武器。旗下网络空间力量的基本指挥关系包括：

- （1）指导全球信息栅格的作战和防御；
- （2）针对特定的网络空间威胁，制定应对方案；
- （3）在创造跨责任区的网络空间效果之前，配合其他的作战司令部和相应的政府机构；
- （4）根据指示，向美国国家机构、商业实体及国际组织提供网络空间方面的军事代表；
- （5）倡导网络空间能力；
- （6）整合战区安全合作活动、部署网络空间作战能力，协同全球指挥与控制系统，向国防部部长提出优先建议；
- （7）做好行动环境中的情报准备，根据需要，和全球指挥与控制系统同步执行；
- （8）依据指示执行网络空间行动；
- （9）根据需要策划、协调以及进行动能和非动能全球打击。

美国网络司令部主要负责指导美国国防部信息网络的运行和防护，负责计划、整合和统一协调网络空间行动。主要职责有：

(1) 统一协调各军兵种联合网络空间作战。作为美军网络空间作战方面的最高管理部门，负责整合各军种网络战资源，协调全军联合网络战模式，做好“顶层设计”，重新调整网络空间作战方式，提高网络空间作战水平，统一从军费中划分款项给各军种实施网络空间作战，协调网络空间作战人员的招募、培训和设备的采购、分配和使用，建立能够使各种网络空间作战能力互相配合的指挥系统，并制定网络空间作战条令和作战计划等。

(2) 实施网络作战指挥。主要实施三种网络空间作战的指挥：一是秘密资料的窃与防。通过查找漏洞、破解密码，窃取机密信息，同时防止己方信息被他方获取。二是网络舆论战。运用新闻传播规律和对敌方社会心理的了解，编造谎言、制造恐慌和破坏团结等，形成对敌方民心士气上的破坏力。三是直接网络对抗。

(3) 保护军方网络免遭敌方入侵和破坏，从针对目标看，美军当前的潜在战略对手，有形的国家是中、俄等竞争对手，无形的组织是反美武装和宗教团体等。

(4) 在网络安全办公室协调下，与政府及民间组织和公司一起，反制敌方的网络入侵。

(5) 对别国网络进行攻击和破坏，争夺网络空间的控制权。

(6) 综合运用技术能力，统一网络空间行动，有效解决网络安全问题，保障网络空间的自由运行，并在保持全球安全环境作战效能的同时，为民间机构和国际合作伙伴提供支持等。

### 2.3.4 美军网络空间作战指挥与控制的关系

根据 2011 年的《统一指挥计划》，美军进一步加强了网络空间作战的全局指控，除美军战略司令部仍保留网络空间作战的指挥外，美国网络司令部在网络空间作战上有绝对的控制权。通过成立网络司令部，美军有效地整合了网络空间防御与攻击作战力量。

图 2-2 为现阶段网络空间作战指挥和控制关系简化模型图。现阶段的网络空间作战指控不再区分全球与战区模式，美网络司令部在攻防两端均具有网络空间作战的集中控制权，具备美国法典 Title 10 与 Title 50 的双重关系。Title 10 方面，军种组成部队包括空军第 24 航空队、陆军网络司令部、舰队网络司令部、海军陆战队网络司令部等军种网络司令部。网络司令部对各军种网络司令部实施作战控制；军种网络司令部通过各作战中心对部署在各战区的军种网络作战组成部队实施作战控制；各军种网络作战组成部队通过网络作战与安全中心（NOSC，Network Operations and Security Center）对战区内各网络作战部队实施战术控制。同时，为了满足各地理作战司令官（GCC）的作战需求，网络司令部通过在各 GCC 的战区网络作战控制中心（TNCC，Theater Network Operations Control Center）嵌入网络支援单元来协调网络空间作战与传统作战行动的关系。Title 50 方面，军种组成部队包括空军情报侦察监视局、海军网络战司令部、陆军情报与安全局、海军陆战队情报局等；美国网络司令部通过国家安全局，对各军种组成部队实施支援和作战控制。

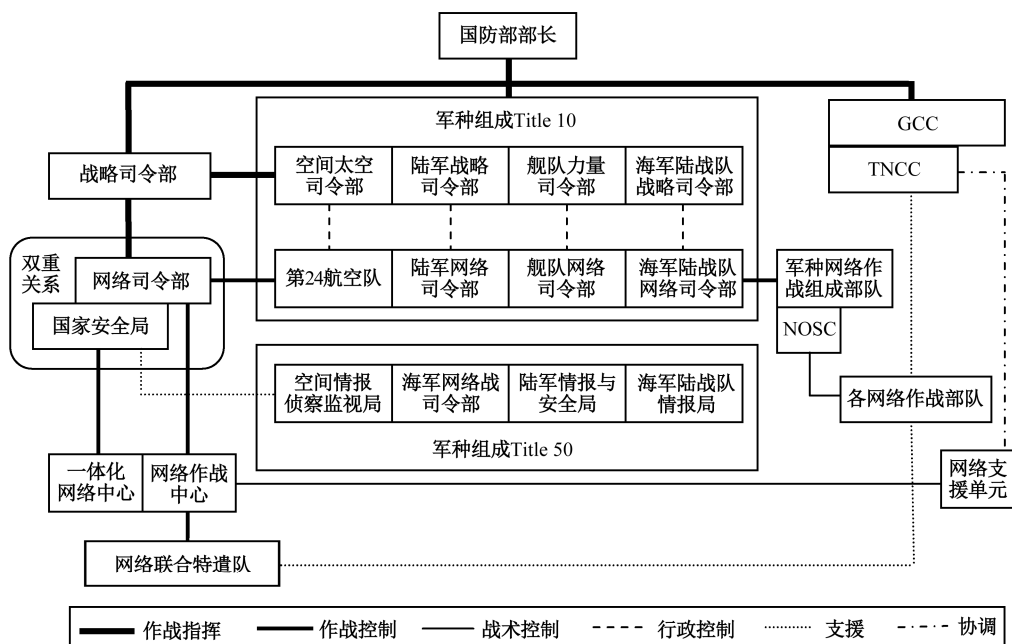


图 2-2 现阶段网络空间作战指挥和控制关系简化模型图

如何理顺网络空间作战的指控关系，是组织实施网络空间作战军事行动首先要解决的问题。美军认为，为了有效地研究网络空间作战的指控关系，首先需要确定“谁指挥”的问题，并在此基础上，逐步解决“网络空间作战在哪里发生”，“有多少个部门参与到网络空间作战中”，“各自履行的职责是什么”等诸多问题。为此，美军通过确立网络空间作战的最高指挥机构，自上而下地形成与完善其网络空间作战指挥链。

虽然我军在体制结构上与美军有很大的不同，但是美军网络空间作战指控关系的演变思路，以及其在政策法规、力量构成、体系能力等方面的经验做法，都值得我们深入学习与研究。

美军网络空间作战战略的实施首先带来的就是军事机构的变革。为应对网络空间作战的新态势，隶属战略司令部的网络司令部，指导全军网络空间作战行动，各军兵种也成立了相应的网络空间作战部队，纷纷制定相应的网络作战力量发展规划，形成了以网络司令部为核心的美军网络空间作战力量和指挥体系，如图 2-3 所示。在网络司令部的统一协调部署下，美军网络力量建设进入了飞速发展阶段。2013 年，美国网络司令部提出扩编到 4900 人，2014 年《四年防务评审报告》提出建设 133 支网络任务部队，2015 年《网络空间战略概要》提出国防部首要战略目标是要建设和训练网络任务部队。

美国网络司令部由 4 类人员组成，即作战人员、领域专家、分析人员和开发人员。作战人员负责制定计划，指挥和实施网络空间的进攻与防御行动；领域专家负责网络空间技术方面的事宜；分析人员主要是情报人员；开发人员主要负责设计和修改软件包和硬件。

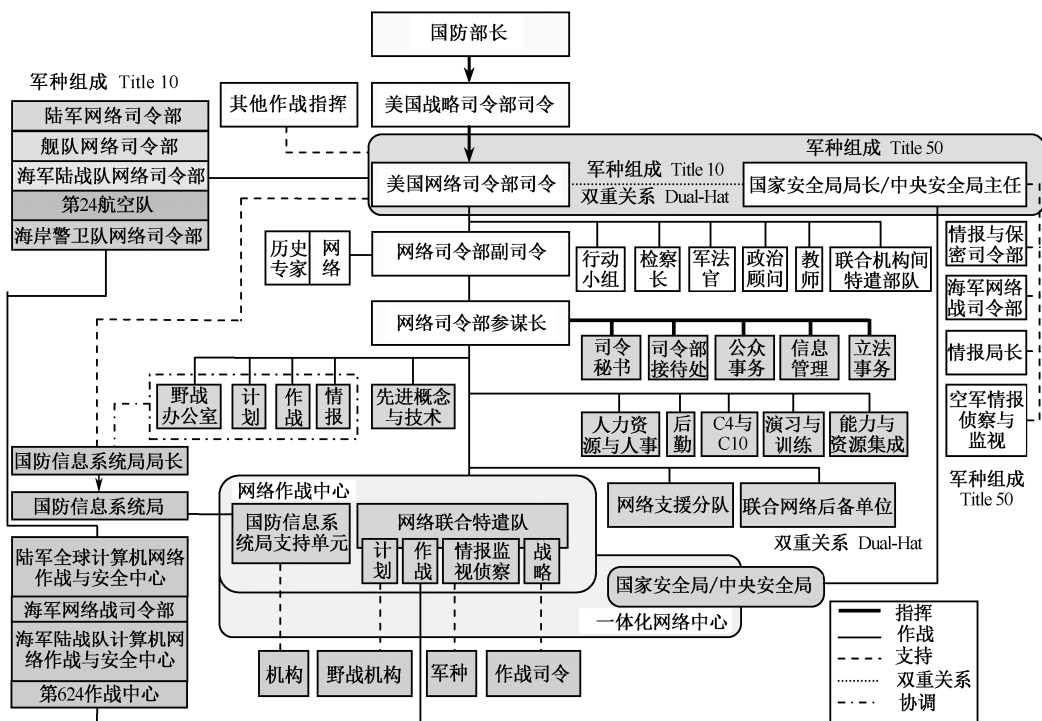


图 2-3 美军网络空间作战力量和指挥体系

### 2.3.5 美国网络司令部的工作重点和使命任务

美国网络司令部面临的工作重点和使命任务体现在以下方面：

#### 1. 整合网络作战力量与资源

美国网络司令部不断整合各军种网络空间作战资源，协调全军网络空间作战模式，成为美军网络空间作战方面掌握实权的职能部门。网络空间司令部要担负起整合、协调军民网络资源的核心使命。这基于 3 个原因：（1）网络空间庞大而复杂，涉及的技术和体系方法随着时间不断改变，网络空间结构也将不断演化，对网络空间的研究需要新技术的持久支持。（2）网络空间作为一个新兴领域，对其内涵的认识虽尚不一致，但在渐进深化。（3）网络空间将成为未来国家所有能力（包括经济、金融、科技、外交和军事能力）的重心。

#### 2. 制定网络空间交战规则

随着网络威胁的不断增加，美军认为需要制定清晰的保护网络空间的规则，来指导对网络攻击的反制措施。尽管美国网络司令部已成立并投入运转，但关于网络空间作战的许多问题并未厘清，如果作战界限不明确将会带来指挥混乱。诸如此类的很多问题将有待深

入系统地进一步研究，否则交战规则的模糊将令美军在面临网络攻击时无所适从。此外，为了充分整合应用网络空间优势，具备实施“攻防兼备”的网络空间作战能力，美军也需要超越在传统单纯机动作战中所确立的规范，制定网络空间交战规则，为形成、发展网络域的实战能力做战术和法律上的准备。

交战规则倡导的是，所有地区性作战司令部的指挥官们具有固有的自卫权利，在条件允许的情况下被赋予自主策划和实施网络空间作战的权限，从而在理论上脱离网络司令部的控制。网络司令部的建立并不会带来交战规则的修改，新的司令部也绝不是一个重复高层命令的单位，它与其他司令部的横向关系，特别是在作战准备环境中的关系，必须仔细加以斟酌。网络司令部作为一个指挥实体机构，联合交战规则对它的运作可能构成一个重大挑战。不应采取任何行动削弱地区作战司令部的权限，但必须颁布一些法律对网络司令部的全球角色加以说明和示例。

### 3. 提升网络态势感知能力

网络空间存在大量攻击的特性，以及敌人在不同的位置可以同时引导这些攻击的能力，使得网络空间司令部提升网络态势感知能力的任务迫在眉睫。除传统部队分清敌友位置及行动的态势感知以外，网络部队的态势感知还意味着，在网络空间这个自然存在而非虚拟、包含事物远比互联网多，而且又具有极端动态、关键弱点和重心瞬息万变的“域”中，要想具备与其他作战相融合的扩展性以及适应性，就必须具备全维态势的感知能力。

### 4. 统一指挥并实施网络战争

从发展趋势看，网络空间作战不再局限于利用网络发起简单的更改网页、侵入敌方计算机系统的攻击行动，而是国家和军队在战略层次上统一实施全面的、联合的和大规模的攻防军事行动。网络空间优势将是美国在其他所有作战领域开展有效军事行动的先决条件。越来越多的作战能力将在这个空间或通过这个空间获得，未来作战将更加依赖网络空间。网络空间作战将逐渐演变成一个完整的战争形态，与核战争和太空战争一样，成为同一战略层次的新型战争样式。网络战争属于国家、战略层次的新形态战争，至少应具备4个条件，即一支统一的网络部队、相当数量的网络攻防武器、系统的网络作战理念、统一的指挥协调机构。因此，统一指挥并实施网络战争将是网络司令部的长期目标。

### 5. 实施网络攻击和网络防御

美军在其联合出版物中关于网络空间作战有如下说明：“网络空间作战就是网络能力的应用，主要目的是在网络空间内或通过网络行动实现军事目标或作战效果。”美军在发展网络防御能力的同时，更加重视网络攻击能力的建设。渗透、监控、利用和摧毁敌方的网络空间是网络部队的重要任务。美军基础能力以及科学技术的深厚积累，能够迅速转化为网络空间优势，确保网络空间作战的实施。目前，在软武器方面，美军已研制出2000

多种计算机病毒武器，具备对网络空间硬载体、软系统进行打击的能力。美国网络司令部通过实施及不断演进网络防御和网络攻击，正在极大地发展并整合各种网络攻防力量，倍增其网络空间作战能力。

## 2.4 美国陆军网络空间作战力量和指挥控制体系

### 2.4.1 美国陆军网络空间作战机构及职能分工

#### 1. 组建作战力量，具备网络空间实战能力

美国陆军从 2010 年开始组建网络作战力量，经过几年来的发展壮大，已经构建了自上而下的网络空间作战指挥与控制体系。

陆军网络司令部于 2010 年 10 月 1 日正式成立，目前已形成完整的作战能力，其职责是：负责陆军全球范围内的网络空间运维；配合美国网络司令部组织和装备网络部队，确定陆军任务需求和部队能力；实施全谱网络空间作战，确保陆军的信息优势；负责陆军全球范围内的计算机应用、网络攻击与防御以及特定电子攻击行动；提供训练有素、准备充分的网络空间作战专业人员，为美国网络司令部提供作战支持。在得到美国网络司令部指令时，陆军网络司令部还将为组建联合特遣部队提供支持；此外，该司令部还负责网络空间陆军部分的态势感知，支持网络空间作战，以使美国网络司令部司令能使用统一的联合网络空间作战视图，实施高效作战指挥控制。

目前，美国陆军网络司令部总部位于佐治亚州戈登堡，计划在全球各地部署约 2.1 万名军人、文职人员和雇佣人员，其下属机构包括陆军网络企业技术司令部/第 9 信号司令部、陆军情报与保密司令部、第 1 信号司令部的部分机构和陆军网络作战与集成中心。网络企业技术司令部/第 9 信号司令部司令兼任陆军网络司令部负责网络空间运维与防御的副司令，下辖 4 个战区信号司令部（分别为美军北方司令部、南方司令部、太平洋司令部、中央司令部、欧洲司令部和非洲司令部提供网络支持）和驻韩美军的一个通信旅；陆军情报与保密司令部司令兼任负责网络作战的陆军网络副司令，指挥所属部队实施网络作战和情报搜集。陆军网络作战与集成中心是陆军网络空间相关活动的指挥控制中心，负责为司令部所属各级人员准确及时地发送命令、向上报告网络空间异常情况，并协调与陆军其他司令部、其他军种网络司令部作战中心和美军网络空间联合作战中心的信息共享。美国陆军网络司令部组织结构如图 2-4 所示。



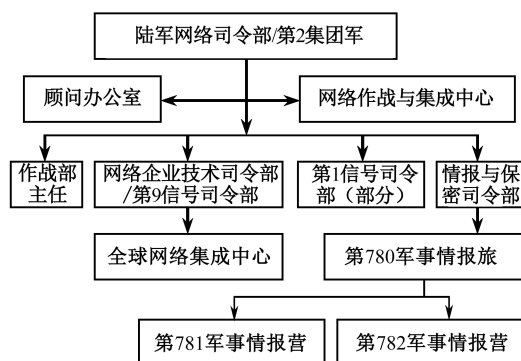


图 2-4 美国陆军网络司令部组织结构

## 2. 发展专业化的网络空间作战部队

在美国陆军网络司令部的指导下，陆军网络空间作战部队规模也在迅速壮大，并已具备实战能力。目前，陆军网络空间作战专业人员已由 2012 年的 6000 人发展到 2014 年年底的 1.4 万人，在 2016 年达到 2.1 万人。

2011 年 12 月，美国陆军网络司令部宣布正式成立专业化网络空间作战部队——第 780 军事情报旅，主要负责实施信号情报搜集和计算机网络战，并负责对国防部和陆军网络实施动态防御。第 780 军事情报旅总部位于马里兰州米德堡陆军基地，编制人数为 1200 人，其中约 80% 为现役军人，其他为文职人员和合同商。该旅下辖 2 个营，分别为驻马里兰州米德堡的第 781 军事情报营和驻佐治亚州戈登堡的第 782 军事情报营。该旅在行政上由陆军情报与保密司令部管理，在作战上由陆军网络司令部直接指挥。

2012—2014 年，美国陆军还新设了加密技术-网络战、网络防御和信息防护 3 个军事技术团队。其中，加密技术-网络战团队（代号 35Q）主要负责军事情报机构的数据安全，计划总人数 500 人，大部分由第 780 军事情报旅指挥和管理，首批人员已于 2013 年 10 月就位。网络防御技术团队（代号 25D）的任务是根据网络空间作战任务评估网络空间潜在的弱点和威胁，计划总人数 600 人，将部署在陆军旅级和师级部队指挥所，首批人员从 2014 年开始训练，2016 年开始部署。信息防护技术团队（代号 255S）将部署在联军司令部、战场信号司令部和战场网络操作中心等核心机构，与网络防御技术团队相互配合，监测网络空间威胁并采取合理的防御和反击措施，计划总人数 250 人，2014 年已部署 60 人。

2014 年 9 月 5 日，美国陆军以驻佐治亚州戈登堡的第 7 信号司令部为基础，启动组建由若干排级分队组成的“网络防护旅”，人员包括士兵、士官、军官和文职人员。美国陆军还在 2016 年组建 41 支网络任务部队，占美军网络任务部队总数（133 支）的 30%，包括网络防御分队、网络作战任务分队、作战支援分队和国家任务分队，将与炮兵、装甲兵和步兵等其他兵种一样作为常规作战力量使用，目前已有 9 支完成组建。

陆军国民警卫队和后备队也将从 2016 年开始组建网络空间作战部队。陆军国民警卫

队已组建了 1 支网络防御分队，最终还要建立 10 支网络防御分队。陆军后备队信息作战司令部改组为陆军后备队网络作战大队，按计划还将部署另外 10 支网络防御分队。

目前，美国陆军的网络空间作战部队已具备实战能力。第 780 军事情报旅的一支特遣队曾在阿富汗协助战区旅战斗队进行网络防御。陆军网络司令部还在西南亚、欧洲、夏威夷、韩国和亚利桑那州建立了区域网络中心，吸收了以前的战区网络作战与安全中心和区域计算机应急响应分队的“操作、维护和防御”功能，这些中心作为战区网络空间行动的联络单位，不仅为陆军提供网络空间作战能力，还与其他军种的战区网络部队协同，为战区司令部提供支持。

### 3. 陆军网络空间作战的职责、任务、重点和原则

《美国陆军网络空间作战能力概念计划（2016—2028）》明确了陆军在网络空间作战的职责、任务、重点和原则，具体内容如下：

#### 1) 陆军网络空间作战的职责

协助美国网络司令部管理和运行全球信息栅格，按照命令执行全谱网络任务，捍卫国家和军队的网络空间安全；及时掌握网络空间内敌友双方的信息，指挥、协调和管理“陆战网”的网络空间对抗与防御能力；支持和协同其他军种的网络空间作战，使美军网络空间作战力量能在全球信息栅格内探测、拒止、压制和击败敌人。

#### 2) 陆军网络空间作战能力建设的任务和重点

美国陆军在网络空间作战中的任务和重点是，不断加强企业级网络对抗能力、网络主动防御能力和网络空间防御工具的研发能力，并将网络空间作战纳入陆军“联合地面行动”体系，支持战略和战术网络的整合，同时提高网络空间作战队伍的数量和质量，建立真实的仿真训练环境，在实战条件下进行联合网络对抗训练。

#### 3) 陆军网络空间作战的原则

陆军网络空间作战的原则，包括各级部队如何在美国网络司令部领导下实施网络空间作战。国家级、联合部队级和陆军级三个层级的网络空间作战由临时组建的部队和作战部队共同实施。通过兵力请求程序，陆军为美国网络司令部、北方司令部、太平洋司令部和所有作战指挥官及联合部队提供训练有素、装备精良、服从指挥的网络士兵，通过组建全球联络小组或支援小组为战术行动提供支持。军级和师级部队由其直属网络行动与安全中心提供建制内的网络空间作战支持。旅级部队由其建制内网络空间作战力量对其网络实施管理和防护，并为其下级部队提供网络防护能力。营级和连级部队分别依靠其上级部队获得核心服务、网络准入与防护能力，且不具备计划网络空间作战的建制能力，仅需执行网络空间作战命令和指挥相关网络行动。



司令部的信息作战司令部。它为美国陆军机构和主要司令部提供跨多学科的信息行动支持，协调信息行动，建立与陆军各机构、海军、空军、参谋长联席会议信息行动中心，以及国防部和国家机构信息行动组织之间的通信联系。

## 2.5 美国空军网络空间作战力量和指挥控制体系

### 2.5.1 空军网络空间作战的组建过程

#### 1. 空军早期的信息战部队

美军各军种中，最早被赋予网络空间作战职能的是空军。1996年8月美国空军组建了研究网络攻防作战的美军第一支信息战部队——空军第609信息战中队，并在南卡罗来纳州的空军基地成立，其55名成员是从受到特殊训练的计算机操作人员和监控人员中择优录取而来的。主要任务是通过下载过去24小时内访问计算机网络的情况来掌握非法入侵信息网络的活动的，并采取有针对性的防御性信息战措施和软件技术手段实施网络防御，保护美国中央总部空军的关键性计算机网络的安全。这是一支专业水平较高的计算机应急响应分队，完全具备向敌方的计算机网络系统发动攻击。

#### 2. “越俎代庖”的第8航空队

在网络空间作战的概念引起美空军重视之前，美国空军兼职负责网络空军事务的是经过重新整合的第8航空队。2002年，作为美国空军信息作战“规范化”的一部分，制订了一项计划，将其情报、监视和侦察（ISR）飞机都集中到第8航空队，为实施网络中心战奠定了基础。

在此之前，2001年2月1日，驻扎在得克萨斯州莱克兰德空军基地的空军情报局（AIA）已经由一个野外作战局变成一个第8航空队下属的单位。而莱克兰德空军基地的第67信息战联队（后改为第67网络战联队）和马里兰州的米德堡空军基地的第7情报联队也先后隶属于第8航空队。这样的调整使第8航空队成为了单一的信息作战部队。

此后又有几支空军ISR联队隶属于第8航空队，包括：内布拉斯加州奥弗特空军基地装备有“铆钉”联合监视系统的第55联队；加利福尼亚州比尔空军基地装备U—2（随后还装备“全球鹰”无人机）的第9侦察联队；佐治亚州罗宾斯空军基地装备“联合监视目标攻击系统”（JSTAR）的第93空中控制联队；俄克拉荷马州廷克空军基地装备有机载预警和控制系统（AWACS）的第552空中控制联队；分别装备EC—130H信息作战干扰平台和机载指挥和控制中心（ABCCC）的亚利桑那州戴维斯蒙塞空军基地的第41和42电子战联队；内华达州内利斯空军基地装备有“捕食者”无人机的第11侦察联队。

经过重组后,第8航空队可以对信息作战进行“从摇篮到坟墓”的管理,包括在网络空军的信息战。第8航空队副司令称,由ISR、指挥和控制、信息作战部队组成的第8航空队可以拥有在全球进行信息战的装备和力量。尽管从装备上看,这支联队距离现在的网络空间作战任务还有很大差距,但是实际上其装备与后来专门执行网络任务的第24航空队非常相似。

### 3. 重组后的第67网络战联队

第67网络战联队司令部同样位于得克萨斯州的莱克兰德空军基地,这个联队是美国空军最大的作战联队,它在除南极洲以外的所有大陆部署有人员和装备。其前身是1993年在莱克兰德空军基地成立的第67信息战联队,2006年7月5日改编为第67网络战联队,成为美军唯一的专业网络战部队。第67网络战联队下辖5个情报大队,35个情报中队及分队,编制人员超过8000人。该联队的驻地分布在全球100个地点,负责为“空军、五角大楼乃至白宫的领导人”提供决策依据。第67网络战联队下属核心作战单位包括驻得克萨斯州莱克兰德空军基地的第67网络战大队。该大队负责为国家决策层提供多种来源的情报、电子战和通信保密技术,同时还为美国空军特种作战司令部提供专门情报。驻马里兰州乔治米德堡的第694情报大队负责实施电子战、保密与信息战,还负责为国家安全局执行任务时提供人员和后勤支援。驻德国拉姆斯泰恩空军基地的第26信息战大队负责为欧洲战区的美军作战部队提供信息战平台,同时还兼顾非洲和中东地区的信息战任务,北约的信息战任务由该大队担负。驻得克萨斯州莱克兰德空军基地的第690信息战大队也是第67网络战联队的骨干。整个第67网络战联队的具体任务包括执行电子战、信息战、网络攻防、应急作战、特种战等。

### 4. 半路夭折的网络司令部

2006年,频频爆发的网络攻击事件引起美国军方对网络空间作战前所未有的重视。然而在那时,美国军方尚没有一个部门来统一负责网络空间的作战。由于作战方式的特殊性,美空军敏锐地看到了网络对于现代作战的重要作用。在2006年美空军颁布的《空军战略计划》中,明确把网络空间正式界定为一个新的作战领域,美国空军提出了掌握天空、太空和网络空军控制权的概念。在这一年的11月2日,美空军部长宣布将设立空军网络司令部(暂编)。根据最初的计划,空军网络司令部于2007年夏天建立,但是后来推迟到2008年年底。根据计划,空军网络司令部将集中第67网络战联队以及第8航空队的其他资源,在威廉姆·T.罗德少将的领导下工作。前空军部长米歇尔维尼将空军网络司令部的任务概括为:“发展成为一个与航天司令部和空中作战司令部并驾齐驱的一级司令部,作为一个‘力量提供者’,确保总统、指挥官和中国人民能够在天空、太空和网络空军自由的行动和完成商业活动。”

根据计划,美空军决定采取分布式结构组建网络司令部,在路易斯安那州巴克斯代尔空军基地保留一个临时性的司令部,同时在全国军事基地分布541个具备实战功能的子司令部。

2008年3月21日的美国《空军时报》披露了计划中的美空军网络司令部编制架构,

网络司令部包括 65 个空军中队、预备役和国民警卫队。此外，还有 4 个空军联队，其中新设立的和在编部队各两支。新设立的第 450 电子作战联队位于得克萨斯州莱克兰德基地，负责提供作战行动支援，配备 EC—130J 等电子战飞机，帮助地面部队防御电子攻击，干扰敌人的雷达和通信系统，帮助本国轰炸机和战斗机突破敌方防空系统。另外，新设立的第 689 网络战术联队位于伊利诺伊州斯考特基地，担负通信和情报作战任务。这两个联队可确保网络司令部按时形成初始作战能力。还有两支在编部队——第 688 信息作战联队和第 67 网络作战联队，与第 450 电子作战联队同样位于莱克兰德基地。在司令部对其进行重新整编后，两个联队将具备空军信息战中心和网络防御部门的功能。

这之后，美国空军紧锣密鼓地展开了司令部组建准备工作。不过“天有不测风云”，由于美国空军发生一系列核事件，空军部长维尼和参谋长莫斯利被免职。随着空军领导层“大换血”，美国空军的网络空间作战发生变化，2008 年新任空军参谋长施瓦茨宣布，空军成立网络司令部一事暂停。2008 年 8 月 14 日，空军发表一份声明，暂停空军网络司令部的组建工作。2008 年秋季，施瓦茨宣布空军航天司令部下设的一个编号航空队取代网络司令部。

## 5. 新生的第 24 航空队

美国空军停止组建网络司令部，并不代表新一代领导人对网络空间不重视，美国空军“仍然热衷于提供全方位的网络能力”，包括全球指挥控制、电子战、网络防御和攻击，只不过是换了一种方式而已。2008 年 10 月 6 日，正式宣布第 24 航空队为空军网络司令部的主体，将网络战大队（第 67 网络战联队）和原临时网络战司令部及其职能归并到第 24 航空队。2009 年 5 月 14 日，美空军宣布莱克兰德空军基地被选为第 24 航空队的司令部驻地。2009 年 8 月 19 日，第 24 航空队正式成立，这也使第 24 航空队成为美国空军最年轻的航空队。

起初，在第 24 航空队内，有超过 7600 名人员支援或者执行 24 小时的网络空间内的行动，这其中包括 3339 名军事人员、2975 名文职人员和 1364 名合同制工作人员。而其所属联队的人员则超过 10 000 人。第 24 航空队下辖 3 个航空联队，其司令机关主要部署在得克萨斯州莱克兰德空军基地和乔治亚州罗宾斯空军基地。其中第 688 信息作战联队是在空军信息作战中心的基础上组建的，司令部位于莱克兰德空军基地。第 688 联队包括 1000 名文职和军事人员，是美国空军负责信息作战的中心。这支联队负责“通过探索、发展、应用和转换信息对抗技术、战术和战略，为作战部队形成信息行动优势，以控制信息战场空间并提供世界最好的信息作战指挥官”。

第 689 战斗通信联队司令部位于乔治亚州罗宾斯空军基地，主要任务是负责美国空军的网络基础设施建设，同时负责通信系统、信息系统、空中交通管制以及提供天气服务。这支部队的人员超过 7000 人，其中包括美国国民警卫队人员、预备役人员和合同制工作人员。

第 24 航空队是美国空军第一个赋予单独的网络空间作战使命的航空队。按照美国空军的说法，第 24 航空队将在网络空间内执行全方位作战任务。其主要任务是向作战指挥官提供训练有素的、预有准备的网络部队，以计划和实施网络行动，并且扩展、维持和防御全球信息格栅中的空军部分。但是从其编制和装备来看，这支部队能够在各种类型的网络中执行攻击任务，如果他们愿意，他们能威胁任何一种网络。

## 6. 其他空军网络作战力量

除以上机构和部队外，美空军还有一些与网络空间作战相关的作战力量。他们大多隶属于空军野战局。空军野战局是空军直属司令部的直属部门。这些网络空间相关作战力量包括空军情报监视侦察局、空军频谱管理局、空军网络空间联合中心、空军网络联合中心等。

### (1) 空军情报监视侦察局

前身为空军空中情报局，2007年8月，命名为空军情报监视侦察局。该局与网络战关系最大，直接向空军副参谋长报告执行情报、监视、侦察和信息等情况。该局编有1.49万人，部署在全球72个国家，下属单位包括航空侦察局、第70 ISR联队、第480 ISR联队，以及空军技术应用中心。同时，它还支援空军网络司令部的第67网络战联队的网络空间作战行动。

### (2) 空军频谱管理局

空军频谱管理局为空军计划、提供、防护、访问、使用电磁频谱，为国防部在国家政策目标、系统部署和全球作战方面提供支援。该局负责开发并实施频谱使用指导方针，撰写空军任务支援手册，并在国防部、个人用户、联邦政府用户之间协调频谱冲突事件。同时，该局拥有认证和频谱授权，能够操控卫星、地基移动无线电、应急无线电、雷达、制导武器系统的能力，还为频谱管理专业职业教育提供职能管理。

### (3) 空军网络空间联合中心

该中心负责设计、开发、维护和集成网络空间各种环境，主要包括两个野战分队：空军指控实验室和空军控制培训与创新中心。2007年4月2日，该中心被指定为空军网络空间联合中心，标志着空军指控重心向网络空间转移。

### (4) 空军网络联合中心

目前，空军网络联合中心隶属于第24航空队，不再隶属于野战局。空军网络联合中心通过招标、评估和确认为空军提供核心网络集成、架构、分析及其他网络相关保障。同时，该中心为空天指挥控制提供无缝连接环境。同时，通过不断改进标准、架构、政策和条例等指导性文件，该中心为空军作战人员提供信息优势解决方案，并具体负责为空军各种通信和信息系统提供设计、测试、训练、实施、维护和资源管理等保障。

## 2.5.2 空军网络空间作战的指挥关系和使命任务

### 1. 指挥关系

实际上，空军第24航空队代表美国空军网络司令部行使职权，通常要负责附属部队的作战控制。第24航空队隶属于空军太空司令部，下辖第688信息战联队、第67网络作战联队、空军网络集成中心和第689作战通信联队（第15作战通信大队），并得到空军情报、监视与侦察局的直接支援。美国空军网络司令部即第24航空队的指挥关系如图2-6所示。

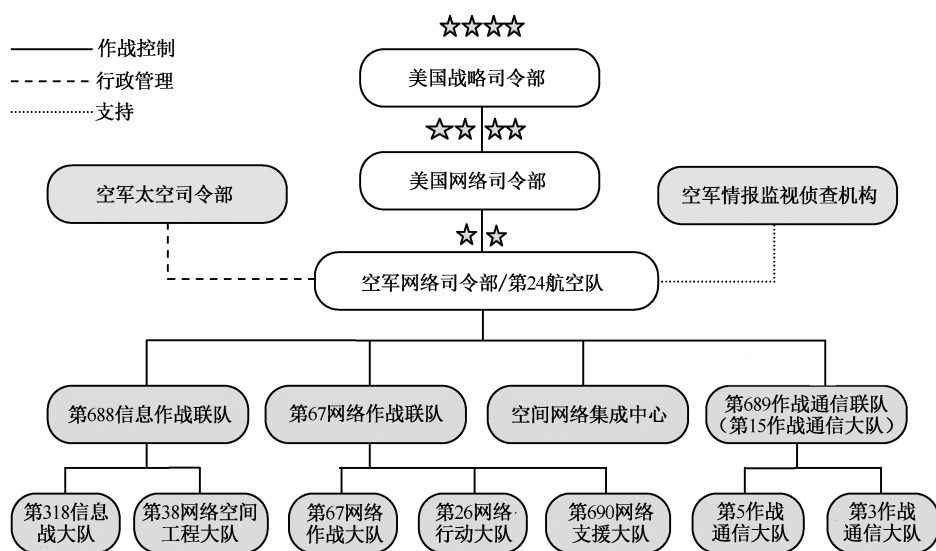


图 2-6 美国空军网络司令部/第 24 航空队的指挥关系

空军组织、训练并装备其网络力量，帮助作战司令官和联合作战人员，并履行本身的职责。网络空间联合部队是军事行动中的一个主要组成部分，而指挥关系是确保及时有效部署的关键一环。美国战略司令部司令主张、策划并执行网络空间行动，有责任为当前的及计划中的联合作战协调、整合网络空间作战，并优先发展，化解冲突。同时空军还会向战略司令部司令提供一些网络空间力量，以进行日常运作。美国北方司令部和太平洋司令部的网络空间作战则负责保护关键的基础设施，民事支援及本土防御任务。空军的网络空间力量和所有的空军部队一样，都会根据需要，被分配给其他的作战司令官、盟军或联合部队指挥官。

## 2. 空军网络空间作战部队组织的使命任务和职责

### 1) 空军太空司令部

空军太空司令部负责组织、训练和装备空军的网络空间部队，执行持久的网络空间作战行动，并全面对接空、太空作战。其作用相当于空军网络空间行动过程和概念的一级司令部。和负责空军网络空间部队的勤务指挥官相同，空军太空司令部的指挥官负责现役部队的行政管理控制并指导预备役空军网络空间部队的行政管理控制，包括网络司令部附属的那些空军——第 24 航空队。而附属空军网络空间部队的作战控制将由战略司令部司令来指导，通常经由美国网络司令部的指挥官到空军第 24 航空队的指挥官行使指挥权。空军太空司令部还要向网络空间领域中的所有联合作战人员提供支援，建立、维护、防御空军网络空间的功能；利用对手的漏洞，攻击对手的系统，以及为附属的网络空间部队提供指挥和控制。

### 2) 第 24 航空队

一是使命。第 24 航空队的使命是通过持久稳固、先进的网络和网络部队巩固网络空



间的优势。网络空间优势是一种重要的能力，它能够直接作用于空军作战的方方面面。第24航空队为指挥官提供与国家、军队和空军目标相符合的持久稳固的网络空间态势感知，提供在电磁频谱领域进行攻防作战，并与空中、空间作战完全实现一体化。第24航空队也会采用相应的技术，通过网络空间产生响应能力以满足新任务的需求，来应对对手所具有的新能力。最后，航天司令部和第24航空队利用、巩固与加强空军的网络空间能力，提供经过训练有素和装备精良的网络空间作战部队，以满足未来不确定的挑战。

二是战略原则。经美空军战略研究会确定，第24航空队履行空军网络司令部职责时，应遵循的基本战略原则包括：确保部队具有进行与空天作战充分整合的全球网络作战保障所必需的战备水平、训练水平和装备水平；确保稳定和安全地进入网络空间，使用网络设备和系统完成进攻和防御任务，以实现美军及其盟友在整个信息空间的行动自由，剥夺敌军的行动自由。

第24航空队在执行网络空间保障任务时，应坚持的战略要求包括：侦察、监视并利用敌方计算机网络为己方服务；保护美军的计算机网络；为在网络中的作战提供保障；为进行无线电电子战提供保障，定下使用作战力量的战役决心；确保稳定地向用户分发信息；攻击敌方计算机网络；对敌方信息网络和基础设施进行无线电电子攻击；进行旨在对敌实施信息影响的作战；无线电电子防护；组织部队（兵力）进行练习和训练；确保在整个网络空间对敌的信息优势。

三是具体任务。作为行政管理控制指挥系统中的空军网络战指挥官，执行空军部长和空军参谋长下达的空军军种任务，直接为空军的各项作战任务提供战略、战役以及战术级的动能与非动能作战能力；主要实施战略攻击以及空中、空间、陆地以及水面作战；监督士气、救济、安全以及附属部队的安全，建立并维护一个安全可靠的网络，负责空军全球信息栅格的作业、防御、维护及控制。除计算机网络作战和信息作战任务外，还包括确定进行网络作战的程序，即分析网络任务和作战活动领域，制定网络行动保障和支持措施，满足美军在电磁领域反制对手的情报需求，为无线电子设备和管理电磁频谱分配频带（确定工作状态，限制、更换频率等）。

为了组织指挥和管理网络空间的使用，要求：组织和实施网络空间防护措施；完成保护网络、无线电电子防护等防御性网络作战任务；分析网络威胁，为作战空间（空中和地面）的作战准备提供保障；确定防御性网络作战计划任务的优先度；评估网络作战风险；在网络空间中组织监督、分配和确定人员责任；通过作战中心对网络作战中的兵力和武器作战提供指挥保障。

### 3) 空军情报监视及侦察局

空军情报监视及侦察局是负责情报监视与侦察的副参谋长下属的实战机构。它的工作是组织、训练、装备、展示并整合全源情报（例如，信号情报、地理空间情报、测量与特征信号情报、人力情报等）及情报部门的全谱能力。它向各阶层用户提供多源情报产品、应用和服务，并提供信号情报领域的专业意见、信息作战（包括信息保护），获取外国武器系统和技术及条约监测。而对于网络空间，空军情报监视及侦察局充当着国家安全局/中央安全局的空军密码部门。它可以授权获取信号情报的行动。

## 2.6 美国海军网络空间作战力量和指挥控制体系

### 2.6.1 海军网络空间作战力量的组建

#### 1. 海军网络空间作战部队的组建

1995 年,大西洋及太平洋联合指控中心与电子战计划署合并,建立了舰队信息战中心。之后不久,舰队信息战中心升格为海军网络战司令部。2002 年,美国海军在弗吉尼亚州的诺福克基地组建新型“海军计算机事故反应队”,在通信网络的各个地点设置了传感器系统,不间断监视网络运行,发现网络薄弱环节并进行维护,对大量的网络数据进行分析,并提出防护建议。2002 年 12 月,来自包括前海军太空司令部、海军计算机和通信司令部、舰队信息战中心、海军特遣队等 23 个单位,统一到海军网络战司令部指挥之下,这是美国海军最高级别的网络空间作战指挥中心,是掌管海军网络系统、协调情报技术、情报处理、空间需求和海军军事行动的中心机构。2005 年,海军网络战司令部把前海军安全活动小组纳入自己领导之下,司令部的任务也发生了根本的变化,成了海军信息作战、网络和太空的领导部门。2008 年,舰队情报职能司令部并入海军网络战司令部,以提高舰队的情报、监视和侦察能力。同年,美国海军开始整合旗下的信息作战体系,成立全新的联合司令部——圣迭戈美国海军信息作战司令部。海军于 2009 年 4 月又成立了“网络化部队办公室”。

#### 2. 海军舰队网络空间作战部队的组建

海军网络防御作战司令部源于 1995 年的舰队信息战中心的一个部门,在 2003 年,作为海军计算机事件反应小组,成为独立的司令部。后来网络防御作战司令部隶属海军第 10 舰队,2009 年 10 月,美海军将原海军网络战司令部、信息作战司令部、网络防御司令部进行编制调整,成立舰队网络空间司令部/第 10 舰队,作为美国网络司令部下属职能组成司令部及网络空间作战部队,负责为海军全球范围内的网络空间、信息、计算机网络、电子和太空等领域的作战提供支持。

#### 3. 海军拓展网络空间作战指挥机构职能

由于舰队网络司令部职能比其他同类型司令部复杂,其主要作战力量第 10 舰队采用非常典型的海军特遣部队编制结构。其中,海军网络战司令部作为网络特遣部队 1010 (CTF1010) 负责网络运行,其下属部队包括海军大西洋计算机与电信区域主站和太平洋计算机与电信区域主站,为舰队提供网络连接、维护和岸上中继;海军网络防御作战司令部作为 CTF1020,负责网络威胁探测和安防响应;信息战任务则由诺福克海军信息战司令

部（NIOC，Navy Information Operations Command）（CTF1030）负责，下辖圣地亚哥和韦德贝岛的两个分队；舰队和战场作战及密码业务则由佐治亚 NIOC（CTF1050）、马里兰 NIOC（CTF1060）和科罗拉多 NIOC（CTF1080）及其全球分布的下属司令部分别负责协调；此外，海军休特兰信息作战中心（CTF1090）被指定为专门的研发机构。

#### 4. 海军陆战队组建网络空间作战指挥机构

为适应美国网络司令部的统一指挥，美海军陆战队已于 2010 年 1 月 21 日在马里兰州的米德堡组建了海军陆战队网络司令部，作为美国网络司令部的下属指挥机构。

海军陆战队网络空间司令部的建设内容包括：建立行之有效的网络空间组织结构；将网络空间资源划分为专业型和相关型。专业型网络空间资源包括作战司令部组织的网络空间行动、海军陆战队网络空间司令部的指挥要素、海军陆战队网络作战安全中心，以及海军陆战队密码支援营 L 连。相关型网络空间资源包括海军陆战队内用于支援以及影响海军陆战队网络的信息技术，而这些资源不隶属于海军陆战队网络空间司令部。当前，海军陆战队正在对这些资源的使用情况进行总结评估。

海军陆战队的网络系统由驻地网络和战术网络组成，它们由海军陆战队网络作战和安全中心负责管理。这两个网络最重要的部分是海军陆战队安全互联网协议路由网络，通过它可以访问美国国防部可互操作的指挥控制数据网络，支持协同的作战规划以及其他作战应用。海军陆战队全球网络的管理分成 4 个区域，分别是首都区域、大西洋区域、太平洋区域及其预备队区域。每个区域由一个区域网络作战与安全中心负责管理该区域网络的安全。跨区域的安全问题，由海军陆战队网络作战和安全中心负责管理。这 4 个区域下辖了 8 个子区域，所有海军陆战队基地和驻扎部队的网络都归到这些子区域中进行管理。这 8 个子区域分别是海军陆战队总部、首都、东海岸、西海岸、预备队、中太平洋、西太平洋和欧洲区。每个子区域都由 1 个海军陆战队信息技术保障中心负责管理，为该区域驻守的海军陆战队提供 IT 服务。

### 2.6.2 海军舰队网络空间作战主要机构的职责、使命任务和指挥关系

#### 1. 海军舰队网络空间司令部/第 10 舰队

海军舰队网络空间司令部的主要职责是：指导海军全球的网络空间行动，威慑并挫败入侵，确保行动自由，为海军全球范围内的网络空间、信息、计算机网络、电子和太空等领域的作战提供支持。

海军舰队网络空间司令部的主要使命任务是：根据美国网络司令部指示，执行网络行动任务，对海上及海军陆上部队进行网络空间作战支持，建设并维护海军作战网络，以及协调海军与其他军种的网络空间作战行动；指导、运行、维持、防护海军部分的全球信息

栅格系统，并确保安全，提供一体化的网络、信息战和空间作战能力；提供海军的全球网络运行态势；开发、协调并评估海军的网络空间作战需求。

海军舰队网络空间司令部新的战略规划提出了五大战略目标：

一是将网络作为作战平台，使对手不能成功攻击美国海军网络；

二是获得特定信号情报，确认提供的信号情报能够及时满足其任务需求，必须能持续提供国家安全局/中央安全署所需的信号情报；

三是通过网络空间传递作战效能，以支持网络空间、电磁机动和信息作战的全频谱作战；

四是建立共享的网络态势感知机制，建立共享的网络空间通用作战视图，使美国海军对各种网络状态以及在其上发生的事件保持快速感知能力，并确认其能够以全球或地区视角，监视海军的网络和通信运行状态、可疑网络行为，并且可以利用这些信息制定网络策略；

五是建立并不断完善海军网络作战部队，建立 40 支高度专业的海军网络行动分队，并制定计划使这些分队持续发展成熟。

海军舰队网络空间司令部设在马里兰州的米德堡，除海军网络战司令部（下辖网络和航天作战司令部和海军计算机与电信地区主站）以外，海军网络防御作战司令部和海军各信息战司令部/网络特遣部队也都将隶属于舰队网络空间司令部。此外，海军作战部第 2 分部（即海军情报局）与负责通信网络和相关信息技术的第 6 分部等部门予以合并，以利于对网络空间司令部诸多职能实施集中统一的领导。

海军舰队网络空间司令部/第 10 舰队指挥结构如图 2-7 所示。

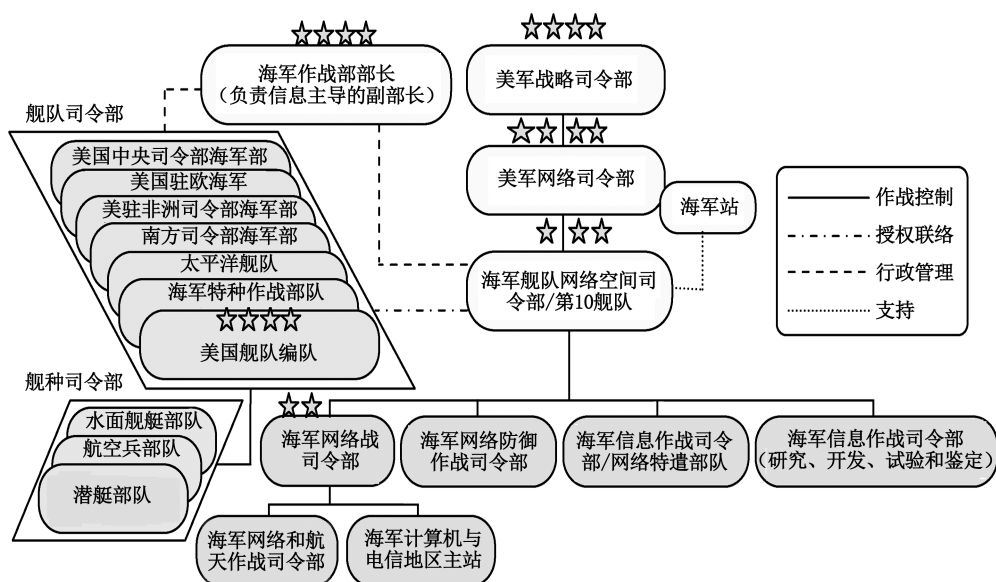


图 2-7 海军舰队网络空间司令部/第 10 舰队指挥结构

## 2. 海军网络战司令部

海军网络战司令部职能和使命主要包括以下三个方面：

一是网络管理。为进行各种军事行动中的作战人员提供信息行动、网络行动和网络空间中的综合网络任务能力，负责海军网络的开发、运作、维护以及安全，协调并评估海军网络、指挥和控制、信息技术、信息行动和空间的作战需求。

二是网络作战方面。为作战部队在信息技术、信息行动和空间的发展和运用上提供支援；能够提供作战行动和技术指导，支持联合特遣部队或军种任务需求，确保舰队指挥控制、通信、计算机、作战系统和情报的安全，保证网络相关系统的可用性，并协调海军内外资源，支持海军部队全球部署时所需的网络基础设施。

三是航天方面。该司令部同时兼任海军航天作战局，在航天方面负有多重职责，包括：海军航天人员配备、部队训练和装备保障；航天领域人才培养；对海军舰队司令部提供航天作战组织领导；以及制作并分发海军航天空间态势。

该司令部下辖海军网络与航天作战司令部、舰队信息战中心、海军特遣部队网络防御中心和海军计算机与电信地区主站。海军网络战司令部编入舰队网络空间司令部之下后，保留其网络和空间作战行动职能，其人力、训练和装备职能移交到舰队司令部，其通信管理职能则移交到海军作战部长办公室。海军网络战司令部从 2002 年发展到今天，已经具有了 15 000 人的规模。

## 3. 海军网络防御作战司令部

海军网络防御作战司令部负责建立和管理海军网络和计算机网络防御，它还肩负保卫海军网络和为联合指挥官保障信息安全的特殊职责。海军网络防御作战司令部目前是国防部唯一一个具有三级计算机网络防御服务提供者资格的单位。海军网络防御作战司令部的工作人员监视着海军及海军陆战队的网络，包括海军及海军陆战队内部网和战术网络，这些网络分布于 16 个国家的 300 个基地，拥有 761 000 个用户。海军现在每年用于计算机系统防御的费用高达 10 亿美元。

海军网络防御作战司令部的另一主要工作是将美国海军的 4 个主要网络：海军陆战队内部网、美国大陆外海军企业网、联合规划网和军医局域网合并到一个中央知识库中，以便对数据进行集中收集和分析。

## 4. 海军信息作战司令部

作为第 10 舰队的职能部门，海军信息作战司令部在美国国内及海外多处部署，主要任务是为美国海军、联合作战部队和其他国家机构提供计算机应急响应、网络脆弱性分析、信息设备防护、信息作战支持；提供信息设施、装备和人员；具体指导信息防御作战，对网络攻击进行探测；各分部任务侧重各有不同。其中休特兰信息作战中心负责信息作战研究、开发、试验和鉴定。

### 2.6.3 海军舰队全球网络作战指挥与控制

海军和空军一样，不再把战区当作指挥单位，为了更好地支持全球作战，海军用隶属于海军全球网络作战与安全中心的两个战区网络战安全中心，来协助原有的位于那不勒斯和巴林岛的两个战区海军计算机与通信主站。另外，由于海军的大多数网络作战是在海上进行，所以他们还建立了舰队网络作战中心，与位于美国本土的战区网络空间作战安全中心互为呼应。舰队网络作战中心是舰队进行网络作战的战术切入点，可以为本防区的舰队提供音频、视频和数据等网络服务，并且可以为舰队从一个舰队网络作战中心的辖区驶入另一个辖区的时候提供平滑的信息过渡。多数未分类的网络都是由美国本土的海军-海军陆战队内联网或者美国海军大陆企业网络(ONENET, Navy's Outside the Continental United States Enterprise Network)负责承包运营的。为了适应战场的需求，海军建立了海外海军-海军陆战队内联网——全球网络作战与安全中心来提供全球性的作战支持，同时也建立了隶属于战区网络作战与安全中心的战区网络空间作战安全中心，对各个具体战场提供支持。战区网络作战与安全中心和所在战区作战司令部并没有从属关系。

支持全球海军作战的最基本的组织是海军全球网络作战与安全中心和东西部战区网络作战与安全中心。海军全球网络作战与安全中心汇集了来自战区网络作战与安全中心、海外海军-海军陆战队内联网和海军卫星作战中心的信息，为全球网络作战联合特遣部队提供全球性的指挥控制信息。海军和陆军不同的是，他们没有维持一个隶属于地理性作战司令部的机构。全球网络作战联合特遣部队建立的部队与战区作战司令部之间的支持关系，并没有赋予地理性作战司令部，在海军军部负责的全球信息栅格范围内进行指挥的权力。战区作战司令部的所有指挥请求都必须先经过海军全球网络作战与安全中心的批准。在海军网络司令部组建之后，海军全球网络作战指挥控制/第 10 舰队全球网络管理体系如图 2-8 所示。

第 10 舰队和网络防御作战司令部直接指挥信息作战中心网络防御机构。各信息作战中心网络防御机构再行使对太平洋、大西洋、欧洲和中央四大地区网络作战中心(NOC, Network Operations Center)与安全中心的指挥权，并通过防御性网络作战(DCO, Defensive Cyber Operations)与四大地区 NOC 与安全中心保持协调。网络防御作战司令部还直接控制四大地区的信息作战中心网络防御和 NOC 与安全中心。太平洋地区启用的是下一代企业网络(NGEN, Next Generation Enterprise Network) NOCs，并指挥计算机与电信站使用远东(FE, Far East)地区的 ONENET。大西洋地区启用的也是 NGEN NOCs。欧洲地区的 NOC 启用的是欧洲(EU, Europe)的 ONENET。中央地区使用的是中东(ME, Middle East)的 ONENET。

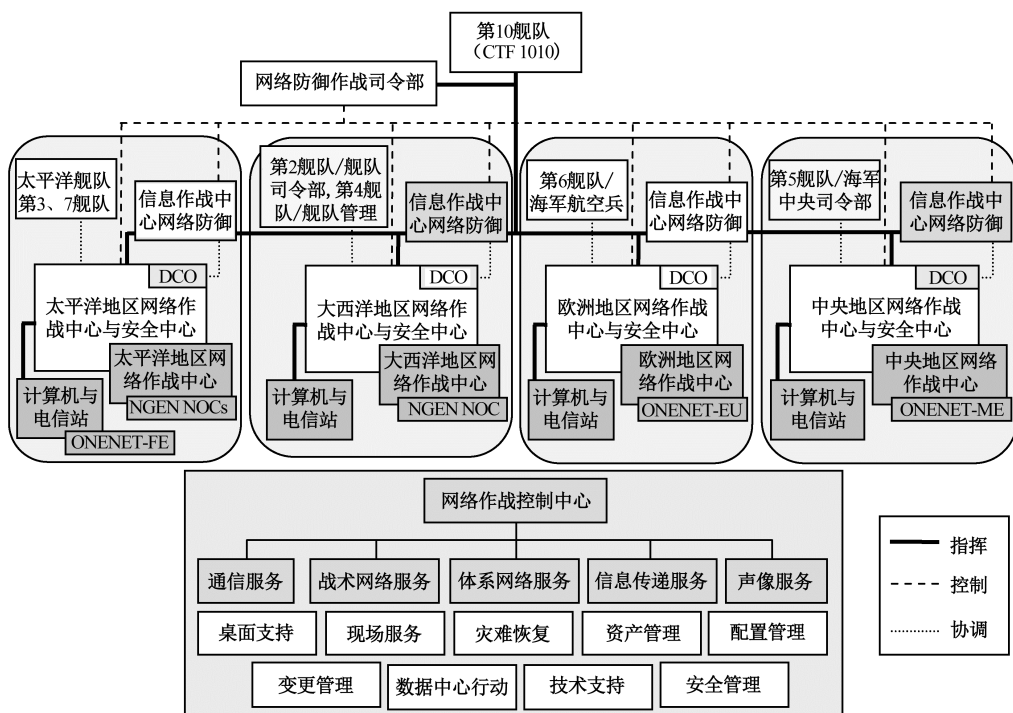


图 2-8 第 10 舰队全球网络管理体系

## 2.6.4 海军陆战队网络空间作战的目的、职责和任务

海军陆战队网络空间作战的主要目的是保护海军陆战队网络的安全，为决策者提供及时准确的信息，使他们能够做出明智的决策，并迅速将作战指令传递给有关部队采取行动。其过程是通过提供能够产生态势共享的 IT 服务，以及相关的技术、过程、工具和组织结构来完成的。

海军陆战队网络司令部主要职责是在美国网络司令部的统一领导下，评估海军陆战队的网络空间作战需求，拟制网络空间作战发展路线图，规划、协调、集成、同步、指导和实施防御性与进攻性的网络空间作战，并保证海军陆战队使用海军陆战队企业网的能力。

海军陆战队网络空间作战的基本任务包括五个方面：海军陆战队网络的管理、海军陆战队网络保证、海军陆战队网络内容管理、态势感知和指挥控制。

### 1. 海军陆战队网络的管理

海军陆战队网络的管理主要用于网络空间作战的监视、管理和控制海军陆战队网络可用性、资源分配和性能所必需的功能和过程。具体包括：服务管理、应用管理、系统管理、网络管理、计算机基础设施管理、卫星通信管理、链路管理、电磁频谱管理。

## 2. 海军陆战队网络保证

海军陆战队网络保证用于保护和防御海军陆战队网络所必需的功能和作战过程。具体包括：网络防御中的应急响应、关键基础设施防护、信息确保能力的管理，以及系统、网络和个人保护信息的政策和过程。

## 3. 海军陆战队网络内容管理

海军陆战队网络内容管理用于监视、管理和支持在海军陆战队网络以及跨网络的信息可视化和可存取性所必需的功能和作战过程。内容管理是指在整个网络系统中统一管理信息的存取，以满足作战任务的需要。内容管理允许信息的使用者订阅所需要的信息，然后通过查找信息数据库检索相应的信息，及时地将其分发给指定用户，使用户能够在协作的环境中维护、编辑、分类、发现、分发、检索和共享数据。

## 4. 态势感知

态势感知是网络空间作战的一种重要能力，目标是实现网络、服务及应用状态的信息共享。态势感知有助于提高网络使用、保护和防御的协同决策，是实现指挥控制的关键。

## 5. 指挥控制

指挥控制是为了保护网络安全，调动遍布全球的区域网络作战与安全中心，以及陆战队信息技术保障中心，一起参与网络作战行动。

### 2.6.5 海军陆战队网络作战指挥的管理流程

为了使海军陆战队网络作战控制过程更加流畅，网络作战行动更加一致，海军陆战队在现有的指挥功能链上进行了重新组织，建立了海军陆战队网络作战任务指派和报告框架，通过这个框架能够比较好地做到全球作战的集中管理和区域作战的分布式管理。

海军陆战队网络作战指挥控制通过规划、指导、协调和控制相关人员、设备、设施、通信完成作战使命。具体而言，网络作战指挥在技术上要实现网络化和信息共享，在方式上实现态势共享决策优势和部队协调自我同步，在组织形式上采取分布协同作战指挥和并行指挥。

为了保障网络作战任务，海军陆战队重新调整了网络基础设施，并把网络作战环境划分为两个管理领域：战术管理和保障管理，它们之间的作战环境和指挥关系如图 2-9 所示。

### 2.6.6 海军陆战队网络作战组织机构

海军陆战队的网络作战涉及许多组织机构，其相互关系如图 2-10 所示。



美国网络司令部是美国战略司令部网络作战的执行机构，负责规划、整合和协调国防部全球网络作战，网络作战任务按照美国战略司令部指挥官的网络作战行动指令来完成。

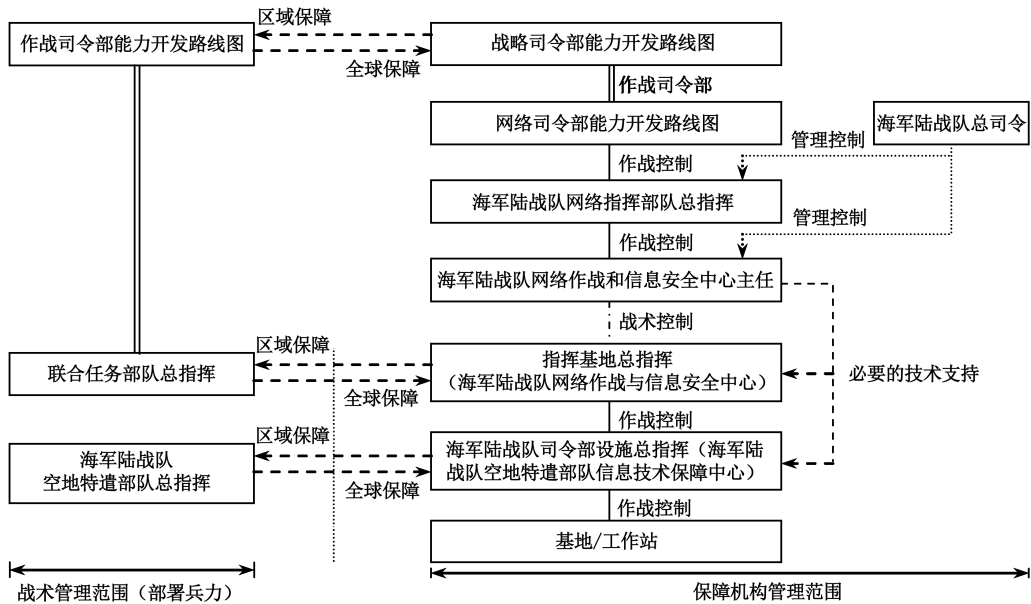


图 2-9 作战环境与指挥关系

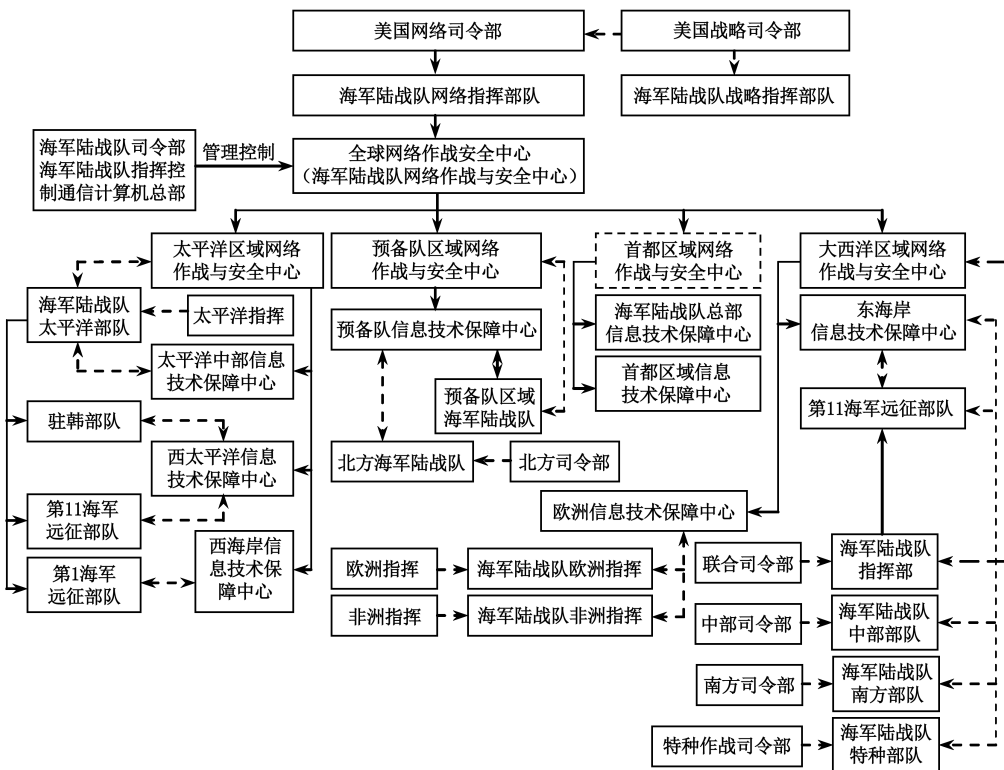


图 2-10 网络作战的作战指挥、海军部队和保障机构之间的相互关系

海军陆战队战略司令部是美国战略司令部的军种部门。虽然海军陆战队战略指挥部不是网络作战指挥链的一部分，但其在海军陆战队网络作战中发挥极大的作用。

美国网络司令部是美国战略司令部的下属单位，在美国战略司令部指挥官的授权下提供全球信息栅格的指挥与控制，在战略、战役和战术层面全方位支持国防部作战、情报及其他业务工作。美国网络司令部负责识别和解决影响全球信息栅格能力的计算机安全问题，支持国防部长办公室、军种、联合参谋部、作战司令部和作战人员。

海军陆战队网络司令部是美国网络司令部的军种部门，负责规划、协调、整合、同步和直接防御网络空间作战。

海军陆战队指挥、控制、通信和计算机司令部为海军陆战队互联网协议路由网络的安全提供战略、政策和宣传，同时保障海军陆战队的联合作战的互操作性。

海军陆战队网络作战与安全中心指导海军陆战队安全互联网协议路由网络的全球网络作战和网络防御，并提供无缝信息交换技术的指导，以支持海军陆战队全球作战，同时它还负责情报的搜集和分析。

其他重要机构还包括前面已经提到的区域网络作战与安全中心和负责子区域网络安全的全陆战队信息技术保障中心等。

## 2.7 美军网络空间作战人才的选拔、培养与模拟训练

### 2.7.1 美军网络空间作战人才的选拔

2011 年，美军制订了《网络安全教育战略计划》，将军队网络人才界定为信息技术安全系统设计人员，网络技术支持、管理和保障人员，识别、分析和处理网络威胁事件人员，网络情报收集人员等类型。依据这一标准，美军遴选网络人才对象扩展至具有法学、心理学、教育学、情报学、政治学等学科背景的求职者。美军为了拓宽网络人才选拔范围，一是将提升网络空间能力的核心要素由技术转向人，强调人才是保障网络安全的关键；二是将衡量网络人才的标准由文凭转向能力，注重选拔人才的专业素质，而不与其学历或毕业院校挂钩。

美军在网络空间作战人才征召和选拔上主要采取以下四种途径。

#### 1. 社会征聘招募

美军在公开的媒体中刊登广告招募“网络真人”，公开招募选拔地方技术人员参加网络空间作战部队，他们的目光还瞄准了众多去微软、谷歌等硅谷 IT 公司求职的年轻技术专家。由于相关待遇优厚，很多技术人才开始加盟政府的“网络黑客”队伍。

## 2. 精确人群征召

每年在赌城拉斯维加斯举办的全球黑客大赛,以及其他各种国际性的黑客竞赛成为美军选拔网络部队人才的天然土壤。谁能在最短的时间内攻陷市面上最强的杀毒软件,谁就能赢得高额奖金和“超级黑客”的称号,同时还可能在美国军方谋得一份薪水可观的工作。据《福布斯》杂志透露,美国军方正在开发一项以前从未有人染指的资源:大、中学生中的网络极客。2009年5月8日,美国军方宣布了一个被称作“挑战网络”的系列网络竞赛项目,倡议书发布在白官网站上,正式向美国年轻人发出号召:“学生黑客、骇客、极客们,山姆大叔需要你们。”该系列赛包含三个针对中学生和大学学生的全国计算机竞赛,旨在发现其中的网络奇才。竞赛将测试学生进攻防守数字目标、盗取信息,以及追踪发现信息盗取者等技能。此次活动的目标是发现10 000名网络人才。

这三项赛事具体为:第一项赛事由美国空军主办,名为“网络爱国者”全国中学生网络防御比赛,重点挑战学生网络防守能力,参赛者必须要抵御侵入他们计算机的“红军”黑客。第二项赛事是国防部网络犯罪中心挑战赛,由国防部防治网络犯罪中心主办,自从2006年开始该中心每年都组织“计算机取证大赛”,现在将参赛范围扩大至中学生和大学生,主要考察选手追踪网络入侵和修复受损数据的能力。由网络安全培训机构和学校主办的第三项赛事是三个竞赛项目中最有争议的一个,即“网络进攻竞赛”。这项赛事旨在挑战学生发现并利用软件漏洞、摧毁敌方网络和盗取数据的能力。其他的赛事还有全国大学生网络防御比赛、美国网络挑战赛等。

竞赛的优胜者将参加每年暑期举行的训练营,这些训练营由美国军方和私营公司共同出资举办,他们还可以获得在美国国家安全局、能源部和卡耐基—梅隆大学的计算机应急响应中心实习的机会。

## 3. 对于其他国家举办的黑客大赛,美国军方也积极参与

2009年4月12日,由韩国搭台请来全球顶级黑客同台竞技,美军就在现场等着“挖人”。此次黑客大赛包括来自瑞典、西班牙、美国、意大利和韩国的36名参赛者,组成了8个“顶级黑客”小组,在此决一胜负。可以说,只有那些被各国安全部门列入重点监控对象名单的世界顶级黑客,才能跻身决赛选手之列。举办这次大赛的目的,是挖掘出之前未被发现的黑客,在确认其实力后,再培养成专家。

## 4. 挖掘校园天才

大中学校校园有潜质的学生人群一直是美军网络战作战人员选拔的关注重点。为了能够在校园中选拔出有天赋的学生,美国军方不惜重金开展相关活动。

此外,美国国防部还推出网络快速追踪计划,以签订商业合同的方式,让网络攻防技能出色的小企业和个人参与其短期项目,从而将民间网络黑客力量也纳入其网络人才队伍。同时也让大型军工企业从中看到无限商机。这些军工企业招兵买马,在利益驱使下积极帮助政府打好这场攻防兼备战。一些大公司表示愿意出资赞助这项系列赛,这些公司都是美国乃至在世界上大名鼎鼎的企业。可以说,目前几乎所有美国最大的军工企业都拥有

与军方和情报机构的网络合同，其中包括诺思罗普·格鲁曼公司、通用动力公司、洛克希德·马丁公司和雷神公司等。

## 2.7.2 美军网络空间作战人才的培养和训练

美国在加强网络空间作战人才选拔的同时，也加强了网络攻击人才的训练和培养。继1995年美军16名“第一代网络空间作战战士”从美国国防大学信息资源管理学院毕业后，又有一定数量的网络空间作战人才相继完成学业，其中还包括一部分信息战指挥军官。1994年，美国成立了信息战战略学院，培养信息战和网络空间作战人才。此外，美国空军军事学院也开始系统培训空军信息战专业军官。

美军在人才培养方面主要做法如下：一是加强网络训练，建立由路由器、计算机、交换机、集线器和天线生成的域，而后加以维护和操作，最终利用这个域实施攻击；二是学习如何在其他用户毫无察觉的情况下，向外部计算机加载恶意软件；三是参加大学网络培训、初始资料培训和任务资格培训，而后对其进行评估考核；四是了解研究网络攻击的成功例子以及其他一些反电子攻击的实验室例子，并能够利用电子战、程序和技术进行阻塞和拦截。

### 1. 广泛实施全民网络安全教育

2010年4月，美国政府启动“国家网络安全教育计划”，旨在提高美国各地区、各年龄段公民的网络安全意识和技能。为推广该计划，2011年8月，美国国家标准与技术研究院发布《网络安全教育战略规划国家倡议草案》。草案明确规定，到2015年，联邦和地方政府以及所有联邦承包商必须采用统一的人才标准，明确网络安全从业人员资质和职业能力要求。

### 2. 培养网络斗士从娃娃抓起

美军培养网络人才的宗旨是在学生群体中普及网络空间作战教育，最终目的是确保美国在日渐激烈的网络竞争中的优势地位，在网络战中稳居攻防主动权。一句话，就是要制海权、制空权、制天权（太空）、制网权一个都不能少。这项活动的动议书甚至将网络空间作战教育与20世纪50年代苏联首颗人造卫星上天，以及之后的美苏军备竞赛中美国政府鼓励青少年积极投身科学研究的情形相提并论，鼓励今天的青少年像当年一样勇于接受网络空间作战的挑战，投身网络事业。

### 3. 完善人才培养体系

美军专门指定由参谋长联席会议主席以及负责计划和资源管理的国防部副部长共同领导美军网络空间作战人才院校的培养工作。目前，美国下一代网络人才正在军事学院接

受训练。如美国海军战争学院、西点军校、空军学院等著名军校，都相继开设了密码学、计算机安全与信息战、网络安全等网络战课程，为本军种培养专门的网络空间作战人才。美国塔尔萨大学设立的网络军团项目，专门训练学生当黑客，课程内容包括编写病毒程序、破解网络密码、攻击网站、恢复数据等。85%以上的学生毕业后进入美军相关机构工作。塔尔萨大学信息安全学院的黑客课程学制为两年，通过课堂理论和实际操作，教授学生跟踪技巧，从垃圾中搜集情报，如何编写病毒程序，借助一系列电子设备破解网络密码、攻击网站、恢复数据等。每名学生会被指定一个警方犯罪实验室，通过实践锻炼黑客技能，学习使用新技术。

2009年之前，美军主要依托国防部信息安全保障奖学金计划，将全国50所军地高校纳入“高水平信息安全教育中心”培训项目，资助信息安全专业的本科生与研究生，并在其毕业后安排至国防部门工作。这一培养模式虽取得一定成效，但培养规模仍受到限制。从2001年到2008年，仅有1001名学生受到信息安全奖学金资助，其中93%最终到网络安全部门就职。有限的资助规模难以满足美军对网络人才日益迫切的需求。

为此，美国国防部一方面扩大奖学金资助范围，另一方面又从2012年4月起联合国家安全局和国土安全部成立“卓越学术研究中心”，将全国145所高校纳入资助培养计划，大幅提升网络人才培养规模。值得注意的是，美军提出网络安全“生态系统”的概念，认为网络人才培养不能局限于以“常春藤”联盟为核心的高等院校，还应积极向中小学拓展。以得克萨斯州的阿拉莫学院培训项目为例，2012年就招收了220名高二学生和168名高三学生参加了信息网络安全学位计划。参加该项目的学生还有机会参观洛克希德·马丁、波音、美国电话电报等公司的一些国防项目。

#### 4. 以多种措施深化专业教育和培训

网络知识在不断发展，要想保持高水平的研究和网络运行队伍，持续学习和技能更新必不可少，为此，美国政府既注重提升工作人员的网络安全技能，又注重培养专业研究力量。例如，将研究型和应用型网络工作人员进行轮换，加强不同领域人员交流，使研究人员更了解实际需求，并实现研究与应用的更好衔接；鼓励政府实验室和机构向参加项目的学生提供实习机会，优先聘用相关学生，并与“政府服务奖学金项目”资助的大学建立合作关系，帮助其开发实用课程、培训计划和实战训练。

#### 5. 网络战士如何训练

为了培养下一代网络战士，美军开发应用的各类军事游戏达百余种，既有利于培训单个人员的单机版游戏，也有用于从班到师级规模的网络版游戏，其中《美国陆军》《全光谱战士》《三角洲部队》《美国海豹特遣队》《使命召唤》《荣誉勋章》等游戏软件，已经成为美军培训专用人才、吸引计算机奇才从军的新平台。为了进一步加强军事题材计算机游戏的开发，美军已投资4500万美元在南加利福尼亚州立大学建立了创意技术研究所，研发尖端的模拟和仿真技术，供军事和教育使用。如何将现有技术应用到实际中是日常训练的重点。

网络战士的训练复杂而奇特。他们的模拟训练更像是科幻小说或计算机游戏情节。他们主要研究两大类黑客攻击——“阻断服务”和“僵尸网络”攻击，而这都是基于真实网络攻击情况的。五角大楼还专门委派了一名将军来负责统率美国的“网上特种兵”。这支部队主要有三方面任务：第一，试验各种现有网络武器的效果；第二，制定美国使用网络武器的详细条例；第三，培训出一支“过硬的网上攻击队伍”。

实际上，黑客部队的训练方法与犯罪分子手法相似。他们主要学习如何在其他用户毫无觉察的情况下，向外部计算机上加载恶意软件，或通过电子邮件、外部光盘，或者在准备好的网址上通过简单的“网上冲浪”来完成任务。

2006年年底，美国国防部还组建了一支全新的部队——网络媒体战部队。网络媒体战部队成员不仅具有较高的计算机水平，而且具有深厚的新闻宣传理论知识。他们既是计算机高手，又是出色的“记者”。这支新军将全天候 24 小时鏖战互联网，“力争纠正错误信息”，帮助美军对抗“不准确”新闻，从而引导利己报道的能力大大增强。

## 2.8 美军网络空间作战演习

美军为了提高网络空间作战能力和人才培养的数量和质量，举行了一系列的演习，其中有的规模非常大，比较典型的有“网络风暴”演习，其规模最大，次数最多，影响深远；“网络防御”演习历史最为悠久，并对其他网络空间作战演习产生了牵引作用和示范效应；“网络闪电”演习向基层延伸；“施里弗”军事演习当中加入了网络空间作战的演习科目；其他的演习还有“虚拟旗”演习、“锁定盾牌”攻防演习、“网络卫士”演习和“网络闪电战”演习，下面分别进行介绍。

### 2.8.1 “网络风暴”演习

“网络风暴”演习是美国国土安全部主办的国家级网络安全演习，每两年举行一次，参演单位来自联邦机构、工业界和外国政府部门。演习内容主要包括：

- (1) 检验参演单位对网络攻击的戒备、防御和应对处理能力。
- (2) 依据国家级政策和程序，演练对网络安全事件的协同响应能力。
- (3) 网络安全事件的态势感知、响应，系统恢复信息的分发和共享。
- (4) 在不损害知识产权和国家网络安全利益的前提下，检查跨行业、跨部门共享敏感信息的方法与流程。

网络空间作战的实战演习，是美国网军建设的重要一环。截至 2011 年，美国已进行了三次大规模的“网络风暴”作战演习，分别为“网络风暴 I”“网络风暴 II”和“网络风暴 III”演习。

## 1. “网络风暴 I” 演习

2006 年 2 月 6 日至 10 日, 在美国首都华盛顿, 上演了一场激烈的大规模的网络空间作战演习——“网络风暴 I”。这场“虚拟网络战争”的规格不同一般, 美国几乎所有的重要部门都动员起来了。白宫国家安全委员会、国防部、国务院、司法部、财政部、国家安全局以及联邦调查局、中央情报局等参与其中; 大名鼎鼎的计算机和软件公司微软、思科、Citadel 和 VeriSign 等倾力相助; 此外, 加拿大、澳大利亚、英国和新西兰的官员也前来观摩。据统计, 总共有 115 家政府部门、私营机构和国际组织参加了这次演习, 而这次战争模拟游戏的“总指挥”则是美国国土安全部。此次演习的主要目的是检验美国的公、私各部门如何应对黑客、博客和反击全球化人士发起的破坏性网络攻击。

这次模拟演习主要是由私营企业设计的, 软件巨头微软、赛门铁克公司等都是演习设计的骨干单位。各企业还派出了高级管理和科技人员参与演习, 包括微软负责网络安全的副主任, 赛门铁克公司的总裁等。演习模拟了恐怖分子、黑客等发起破坏性网络攻击, 导致能源、运输和医疗系统瘫痪, 网络银行和销售系统出错, 软件公司发售光盘中含有病毒等危险。

### 1) 演习的目的

演习的具体目的包括以下几点:

- (1) 演练跨机构协调, 如标准作业程序、通信和决策支援机制。
- (2) 演练跨政府和政府内部协调和事故反应。
- (3) 确定阻碍或支持网络安全要求的政策/事项。
- (4) 确定公共与私营部门接触交流和协调起点, 以提高网络事件反应和恢复能力, 并确定关键信息共享路径与机制。
- (5) 检验、改善和促进公共和私营部门向关键利益相关者及公众发布适当信息时, 在方法和程序方面的互动。
- (6) 确定具有经济和政治影响的基础设施对网络的物理依赖。
- (7) 提高对重大网络事件经济影响与国家安全影响的认识。
- (8) 明确具备网络事件反应和恢复能力的现有手段和技术。

### 2) 演习预案的设置

预案的主要假想目标包括通过网络攻击中断特定的关键基础设施, 阻碍政府对网络攻击做出反应的能力。假想敌是资金充足、具有政治目标的“黑客”松散联盟; 敌方对多个基础设施进行渗透攻击并误导媒体, 旨在发表政治声明, 抗议政府和工业界的行为。攻击者致力于扩大经济危害, 阻断各种服务、误导媒体和其他信息来源, 煽动公众对大型商业机构和政府的不信任。预案具体设置如下:

- (1) 一系列可疑事件引发事故, 迫使州信息安全官联系州长, 要求启动州紧急行动中心。
- (2) 州信息安全官关注的情况包括黑客侵入医疗保险数据库, 可能破坏公众医疗记录。

州政府官员通过与州信息共享与分析中心、美国计算机应急响应小组交流，了解情报部门有关非特定网络威胁的报告，咨询各州信息共享与分析中心后，发现还有 6 个州也出现类似问题；由于受到大规模计算机病毒攻击，某些州服务支持系统崩溃或运行异常。

(3) 评估上述事故后，州长确定威胁是有组织的，非常严重，需要启动州紧急行动中心，并向国土安全行动中心报告。

(4) 多个联邦执法、情报、国土安全、国防和专门部门与其他相关机构协作，减少更多攻击的危害，确认和消除威胁，重建基础设施，恢复公众信心。

(5) 尽管州政府保持了主动权，并成功终止攻击，但信息安全官收到攻击者发出的信息，如果勒索要求得不到满足，类似攻击还会发生。

(6) 受到攻击的州非常重视此次威胁，与联邦调查局协作抓捕敌人，并继续实施网络反应程序。

### 3) 演习场景

位于市中心的美国特别秘密部队大楼的地下室内，几十台计算机高速运转，一支由美国政府组建、训练有素的网络空间作战部队紧张地忙碌着。他们分成两班人马：一部分模拟黑客和博客，通过网络技术甚至物理破坏的手段，大肆攻击美国能源、信息科技、通信与交通部门等关键部门以及著名公司的网站和基础设施；另一部分则负责收集受攻击部门的反应信息，并及时协调行动，制定对策。

这次演习模拟的一个主要场景是：黑客导致十个州的电力供应系统无法正常运转，网络银行和零售系统出错，商业软件公司发售的光盘感染病毒以及核心网络技术存在严重安全漏洞等种种危险情况攻击，“攻击方”发起攻击的次数超过 800 次，有些非常有杀伤力，有些只是各种干扰。被攻击的计算机系统一度出现险情，但由于受攻击一方与指挥部门及时应对，最终使攻击没有得逞。

### 4) 主要成果

此次演习取得了多项重要成果。这些成果包括：

- (1) 首次检验了网络空间在真实危机中可能采用的所有反应政策、条令和通信方式。
- (2) 检验了国家反应计划网络事件附件规定的国家网络事件政策与程序。
- (3) 建立了许多公共与私人关系，这在未来应对跨部门网络事件中将发挥重要作用。
- (4) 通过公共与私营部门协作，确认了需要进一步评估与恢复的事项。
- (5) 在保护物理和网络关键基础设施方面是一个重要的里程碑，达成了参演方和利益相关方的目标。
- (6) 在危机反应的操作、政策和公共事务层面实现了国际协作。
- (7) 对演习的计划、实施和行动进行了系统分析。
- (8) 在联邦机构之间、政府和私营部门之间，以及国际伙伴之间实现了前所未有的合作和信息共享。

美国政府对这次演习的期望值很高，一共投入了高达 300 万美元的费用来筹划和实施



此次规模空前的网络风暴行动。“网络风暴 I” 演习，是提高政府全体应变能力的一次大练兵。

## 2. “网络风暴 II” 演习

美国国土安全部 2008 年 3 月 10 日至 14 日举行了代号“网络风暴 II” 的网络空间作战大演习。这是美国继“网络风暴 I” 后又一次全面检验国家网络安全和应急能力的演习行动，共有国防部、国务院等 18 个联邦机构、9 个联邦州、思科和微软等 40 余家大型科技企业参与，还邀请了英国、澳大利亚、加拿大和新西兰 4 国进行联合演习，规模堪称史无前例。

### 1) 演习的目的

网络风暴 II 演习旨在改善网络事件响应共同体的能力，促进在关键基础设施行业中公共-私营伙伴关系的发展，并且加强联邦政府和其在州、地区和国际层面政府伙伴之间的关系，检查网络响应共同面对通过全球网络基础设施多行业协同攻击响应的过程、程序、手段和组织，协同网络攻击，促使从技术、行动和战略全景方面的事件响应。

- (1) 检查参与组织准备、保护和响应网络攻击相关的能力。
- (2) 依照国家级政策和程序，演习事件响应的高级领导决策和机构间协调。
- (3) 为网络态势感知、响应和恢复信息的收集和分发，验证信息共享关系和通信通道。
- (4) 检查以安全可靠而不危害产权和国家安全利益的方式，跨标准、边界共享敏感和保密信息的手段和过程。

### 2) 演习预案的设置

预案关注三个关键领域，即互联网中断、通信中断和控制系统问题。在演习过程中所有的攻击都是被模拟的，模拟的攻击集中于信息技术、通信、化工和运输（特别是铁路和管道）行业的关键基础设施，参与者可以提出应对相关网络事件的有效解决方案并对网络事件的复杂性和相互依赖性做出评估。

预案的总体设置为敌方联合起来发动经过协调的全球规模网络攻击。

(1) 敌方利用复杂的关系网络协调目标，破坏互联网的连通，中断各行业的运行。敌方特地将几个基础设施部门作为目标，此外还有州和联邦机构、媒体和其他国家。

(2) 敌方利用伪造的数字证书引导“受骗”网站不知情的网络用户，骗取资金和个人信息。对域名服务器和电信路由器的协调攻击导致服务中断和电话通信的不稳定。用户间歇性地不能上网、发送电子邮件或打电话。受攻击影响的人员在通信中断时不得不采用其他通信方式。

(3) 敌方对关键基础设施部门的个别行业进行攻击，目的是利用针对特定目标的集中攻击中断更多的信息和通信服务。

(4) 政府部门受到了协调攻击的影响。在国家层面，敌方渗透在线服务，欺骗本地公民，损害政府信誉。在联邦政府层面，数个机构受到通信中断的影响。比如国防部移动设

备服务功能下降，敏感信息泄露。外国政府受到类似攻击的影响，导致严重的通信困难。随着危机持续，媒体努力发布及时准确的信息。

(5) 事态明朗后，执法和情报部门收集情报并做出必要反应，与受影响的私营部门和其他政府机构协调，努力阻止攻击，恢复对互联网的信心。所有参演机构凭借相互信任的关系，建立新的通信渠道共享信息，形成和传递态势感知情报。

“网络风暴Ⅱ”是一个想定驱动的演习，通过定时的模拟和有计划的注入来刺激满足演习训练目标所必需的预期表演者行动。演习想定是利用具有可信能力的真实和虚构的对手建立的。想定建立于一系列在对手的技术能力范围内置于死地的网络攻击载体。想定没有设定试验系统的技术安全，而是演习响应组织的准备情况与恢复力，和他们跨权限与所有者利益边界有效协同响应的能力。

### 3) 演习场景

此次演习指挥部设在位于华盛顿美国特工处的一间办公室内。来自 5 个国家和 40 家企业的网络专家在演习期间面对约 1800 项挑战，包括黑客入侵、网络欺诈、服务器被攻击等。演习采用特制系统，模拟真实环境中发生过的情况对网络发起攻击，以“检验国家网络安全状况和应急能力”。此外，演习还设置复杂环节，检验美国政府的“绝密”网络安全程序“爱因斯坦”计划。“爱因斯坦”计划用来发现美国所有政府网站上的入侵，并监控网络系统安全。

### 4) 演习的时间筹划

- (1) 2006 年 12 月，召开概念制定会议，确定演习范围和目标，以及计划小组组成；
- (2) 2007 年 3 月，初期计划会议，确定参演单位目标、预案框架和假想敌；
- (3) 2007 年 7 月，召开中期计划会，确定预案要素，分配具体预案制定任务；
- (4) 2007 年 12 月，召开最终计划会议，报告预案事件详细进展情况，制订跨部门事件时间表，确定参演人员、通信方式和数据采集要求；
- (5) 2008 年 1 月，召开最终主预案事件列表会议，推演整个预案，培训现场观察人员和控制人员，完成演习控制程序，制定演习开始前时期协议；
- (6) 2008 年 2 月，演习开始前召开动员会议，根据以往经验准备演习，鼓励公共和私营部门参与。

### 5) 主要成果

各参演单位在安全的环境下评估了自身网络事件反应能力，演练了跨部门协调与信息共享，明确了在网络安全准备方面需要加以改进的领域。

- (1) 加强了网络反应和事故管理部门之间的联系，并建立了新的联系，这对于不断制定有效应对网络攻击的方法与程序至关重要。
- (2) 提升了事故反应中公共与私营部门协作的重要性，突出可加强这种协作的领域。
- (3) 明确了提高网络反应能力的其他协作方式和方法。

(4) 参演单位高层和决策者充分掌握情况、有效参与。

(5) 区分和确认了网络事件与攻击特有的复杂性。由于网络反应的这些特性，需要对国家层次的危机反应模式进行根本调整。

(6) 跨越多个领域演练信息共享能力。

(7) 确定了需要进一步分析、审查和加强的领域与状况，以提高国家网络反应能力。

这次演习耗资 600 多万美元，仅制订预案就耗时 18 个月。与“网络风暴 I”相比，“网络风暴 II”的规模和难度均有所增加。

### 3. “网络风暴 III” 演习

2010 年 9 月 27 日，一场多国、跨部门网络演习在美国展开。演习代号“网络风暴 III”，由国土安全部负责，为期 3 天。其规模和复杂程度超过前两次演习。“网络风暴 III”演习建立在“网络风暴 I”和“网络风暴 II”的基础之上，演习科目的设置反映了网络黑客技术的最新发展，演习中黑客已经不仅仅满足于篡改网页、发起拒绝服务攻击，还瞄准了网络基础设施，破坏人们对电子商务和电子交易的信任感。

7 个美国内阁级政府部门参加演习。除国土安全部外，还有商务部、国防部、能源部、司法部、交通部和财政部。白宫及情报和执法部门代表也参与其中。参加演习的还有美国 11 个州和 60 家私营企业。这些企业来自金融、化学、通信、水坝、防务、信息技术、核能、交通和水资源行业。澳大利亚、加拿大、法国、德国、匈牙利、意大利、日本、荷兰、新西兰、瑞典、瑞士、英国作为国际伙伴参加演习。

#### 1) 演习目的

演习目的在于检验美国重要部门遭遇大规模网络攻击时的协同应对能力；当重大网络事件发生时，为政府机构、私营企业和国际伙伴提供一个框架，使它们具有有效事件反应的能力，实施有效的协调。

(1) 检验新成立的国家网络安全与通信集成中心。该中心是美国网络安全行动的协调中心，集中了美国政府和私营部门的计算机专家。此次演习是这一中心成立后接受的首次重要检验。

(2) 演练新制订的“国家网络事件反应计划”。这一计划由国土安全部牵头，联合政府和私营部门共同制订，旨在发生重大网络事件时，为政府部门、私营企业和国际伙伴提供一个框架，使其有效应对网络事件。

(3) 演练信息共享机制。测试不同机构如何整理、汇总和利用共享信息，尤其是政府机构如何快速处理秘密信息，实现与私营部门的共享，这些部门控制着互联网和其他计算机网络所依赖的基础设施。

#### 2) 演习预案

模拟针对美国政府和国家关键基础设施，如能源网和核电厂的大规模网络攻击。预案反映了对手日益增长的能力，由传统的网页涂改和阻止服务转向有针对性的先进攻击，利

用互联网基本要素攻击互联网。

- (1) 针对互联网基本服务的身份认证系统和域名系统的攻击。
- (2) 设置 1500 起以上的模拟事件。
- (3) 结合对手已知的技术能力，并利用网络基础设施的弱点。
- (4) 攻击使生命受到损失，通信电力系统等重要公共和私营部门运行受到严重影响。

与前两次演习不同，这次演习没有在搭建好的虚拟网络环境中进行，而是首次通过真实的国际互联网实施演习。来自各地的网络黑客通过互联网针对美国政府网络 and 关键基础设施网络实施攻击。但是不会攻击任何真实网络，不会摧毁一个网络，不会输入任何恶意软件。网络攻击是高度未知的、不可预测的，通过演练探索网络威胁下的跨行业、跨部门、跨地区、跨所有权边界和跨国的协调合作机制问题。

## 2.8.2 “网络防御”演习

### 1. 基本情况

“网络防御”演习由美国国家安全局信息保障处发起，美国、加拿大的部分军事院校参加，旨在训练和培养网络空间战后备力量。网络防御演习从 2001 年到 2011 年已经连续举办了 11 届，并对美国“网络风暴”等演习的诞生产生了牵引作用。

在网络防御演习当中，国家安全局组织的红军对各军校学员组成的蓝军发动网络攻击，蓝军全力进行防御，以确保网络的安全和网络服务的正常运行。军校学员根据所担负的不同任务进行分组，比如软件监视组、邮件/即时通信监视组和网络安全监视组。演习后期还包括一个分析项目，学员需要找出国家安全局的安全专家攻陷了哪台计算机，然后针对其所采用的攻击工具撰写一份详细的分析报告，为下一届参加演习的学员积累经验。近年来，网络防御演习的重心有从网络防御转向网络攻击的趋势，红军和蓝军在演习最后一天都将参与对国家安全局组建的网络靶场发动全力攻击。

2001 年，举办了首届网络防御演习，3 所军校组队参赛，分别为西点军校、美国空军军官学校、美国海军研究生学院。2002 年，美国海军军官学校和美国海岸警卫学院加入演习。2003 年，美国商船学院和美国空军技术学院加入演习。2009 年，加拿大皇家军事学院加入了网络防御演习。网络防御演习从而演变成为一项大型跨国网络安全军事演习。

2005 年，参演各方共同制定了网络防御演习指导文件，阐述了演习场景、指挥结构、网络架构、运行服务和交战规则。国家安全局于 2006 年 1 月正式颁布了这个指导性文件。此后，每届网络防御演习均以此文件为指南，根据技术发展和现实需要提出不同的演习主题和场景，加强演习的针对性和创新性。

每次演习结束后，组织者都会从参赛军校当中评选出优胜单位并授予奖杯。在 2011 年 4 月举行的第 11 届网络防御演习中，西点军校队第六次夺得奖杯。

## 2. 参演单位与分工

网络防御参演单位主要有国家安全局、空军信息作战中心、海军信息作战中心、陆军第1信号司令部、海军陆战队网络作战安全中心、陆军预备役信息作战司令部、国家威胁作战中心,以及各大军事院校。其中,许多单位隶属于新成立的美军网络空间司令部。

与传统的演习设置类似,参演单位分为红队、蓝队和白队三方。红队为攻击方,负责对蓝队构建的网络进行入侵和攻击。蓝队为防守方,检测和抵御红队发动的网络进攻,保障网络的正常运行和安全。白队为中立方,对演习进行指挥,并对演习结果进行评估。

### 1) 红队

红队作为攻击方,由来自国家安全局和三军网络作战机构的专家组成。这些专家精通软件漏洞和网络攻击技术,设法运用各种工具猜测蓝军计算机口令字、涂改网页、实施拒绝服务攻击、突破防火墙以及取得蓝军计算机的控制权。演习规定,红队可以自由使用任何公开可用或开源的方法对蓝方网络进行攻击,但不得使用美军开发的秘密攻击技术或工具。

### 2) 蓝队

蓝队作为防守方,由各军校参赛队组成,成员多为计算机相关专业的本科生或研究生。各队在自己的学校构建网络,并采取各种防御措施。在连接起来以后的虚拟专用网上,蓝队防御网络、红队攻击网络,以及白队测评网络。蓝队可以自由选择网络架构,搭建 Web 服务器、电子邮件服务器、交换服务器等,并由队员负责设计网络安全方案,包括防火墙、入侵检测系统、加密技术、深度/广度防御办法,以及灾难恢复措施,然后接受红队攻击。

蓝队要完成白队指定的演习科目,包括查找红队预先植入网络的安全漏洞、陷阱、恶意指令代码并加以排除,检测和击退红队发动的攻击,保持蓝队网络和服务的正常运行。演习结束后,蓝队要按照白队指定的时间和格式,提交网络运行态势、物理安全、脆弱性评估等方面的报告。在演习过程中,蓝队被禁止发动攻击行动,否则将受到处罚。

### 3) 白队

白队作为中立方,由国家安全局和三军的网络作战专家组成。白队驻扎在网络防御演习的指挥中心,对演习进行导演和仲裁,并向每所院校派遣两名评估员。为确保对抗的真实性和公平性,白队不会向红队提供蓝队的设计文档或特定细节。

## 3. 网络演习环境

要成功实施网络防御演习,就需要构建一个真实可控的网络环境,兼顾实战性、可控性、安全性和公平性。在演习环境下,可以试验各种网络攻击和防御方法,可以监测演习过程和评估演习效果,同时还要避免对外部网络如国际互联网造成干扰和影响。

网络防御演习的网络环境构筑在虚拟专用网(VPN, Virtual Private Network)之上,即使需要通过国际互联网,也采用 VPN 技术,从而使演习在一个安全的内网中进行。整

个网络由指挥中心（白队网）、红队网络、蓝队网络组成，通过虚拟专用网连接起来，所有演习数据和流量约束在演习网络之内。图 2-11 所示为网络防御演习的网络架构。

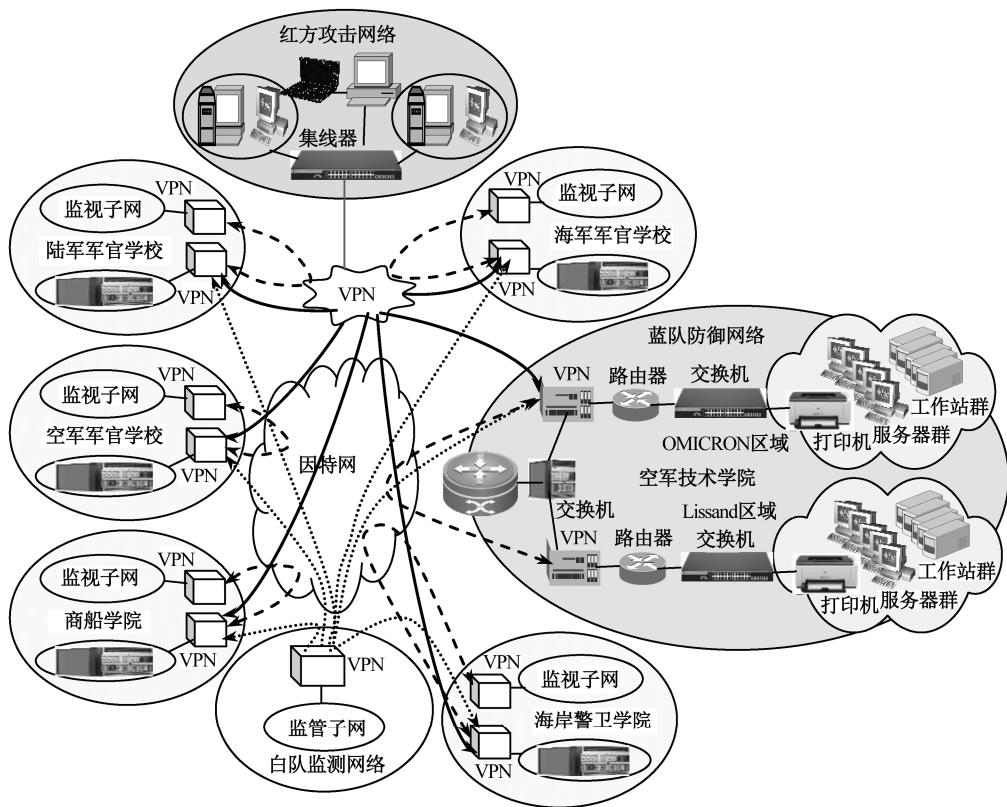


图 2-11 网络防御演习网络框架

国家安全局为网络防御演习提供经费支持，在举办第一次演习时采购了大量服务器、路由器和工作站，为每届演习提供专项经费，并允许每个参赛院校根据需要采购设备，如进行 2006 年网络防御演习时允许各院校购买 4 台戴尔工作站和 1 台思科路由器。在该届演习中，每个参赛院校的防御网络包括 17 台戴尔 PowerEdge 服务器、4 台戴尔工作站、一些思科路由器、支持设备和微软软件及其他开源软件。在演习之前，白队对演习预算进行定制，对第三方采购加以限制，为每个院校提供一些软件。所有使用的软件，不管是自由软件或开源软件，必须得到白队同意后方可使用。所有参赛队均采用大致相同的硬件设备和软件系统，基本能够体现竞赛的公平性。在此基础上，参赛队可以自由选择网络架构，由学员负责计划如何满足对网络和服务的设计需求，例如网络的功能性和可用性，设计网络的安全防范措施，自己安装必要和常用的应用软件，并确保网络系统的安全。

从 2006 年网络防御演习开始，红队在每支参赛蓝队的网络系统中预置恶意软件、后门、黑客工具和木马病毒。表 2-1 为 2006 年网络防御演习当中蓝队系统被预置的各种恶意软件或代码。蓝队运用各种工具检测和清除这些恶意软件和代码，并写出分析报告上报。据报道，为检测和清除恶意代码，蓝队使用了 Rootkit Hunter、f-Prot Scan、Chkrootkit、Rootkit

Reveal、Clam-av、nmap、Icesword、Microsoft Baseline Analyzer 等工具，这些工具都可以从互联网下载。

表 2-1 在 2006 演习当中，蓝队系统被预置的恶意软件或代码

虚 拟 设 备	预置的恶意软件或代码
Web 服务器	2 个可疑目录，2 个后门，2 个木马，2 个可疑系统文件，1 个恶意脚本，1 个恶意网页文件，2 个黑客工具，1 个未授权用户
SMB 服务器	2 个可疑目录，2 个后门，2 个木马，2 个可疑系统文件，1 个恶意脚本，1 个恶意网页文件，2 个黑客工具，1 个未授权用户
XP 客户端 1	3 个不需要的应用程序，2 个木马，2 个黑客工具，1 个后门
XP 客户端 2	1 个不需要的应用程序
XP 客户端 3	16 个不需要的应用程序
Exchange 服务器	4 个后门，1 个木马，1 个黑客工具，3 个错误配置
域控制器	1 个未授权用户，4 个后门，1 个木马，1 个黑客工具，4 个错误配置

4. 演习流程

正式演习时间一般持续 4 天。在演习之前和演习结束后，各方还要做大量准备工作和收尾工作。一般来说，整个网络防御演习流程分为 3 个阶段：

第一阶段为准备阶段，约 45 天。在此期间，网络防御演习指挥部开始运作，组织红、白、蓝等参演各方进行演习筹备工作。蓝方各队按照白方制订的演习计划设计和构建本队的网络，安装所需的软件。

第二阶段为正式演习阶段，一般为 3 到 4 天。考虑到参赛院校不具备 24 小时演习能力，因此定在正常工作时间开展演习，并且每天保留 2 小时作为维护时间。演习开始后，红队启动对蓝队网络扫描，查找漏洞和脆弱性，并开展攻击。白队启动评分系统，对蓝队的防御活动进行评分，蓝队的网络如果发生服务中断或系统、数据被破坏，则将被扣罚相应的分数。

在 4 天的演习进程中，演习按照拟订方案一步一步推进。白队使用电子邮件、电话或由驻扎在蓝队现场的评估员下达指令，启动演习科目。这些演习科目对蓝队网络的程序、策略和计划进行测试，包括新建用户账户请求、检查磁盘文件、向网络上传文件、自然灾害和设备故障应对等。蓝队按科目要求进行响应，竭力保持网络系统的正常运行，迅速排除各种故障。白队则按照蓝队表现和提交的报告，给予相应的评分。

第三阶段为演习后总结和颁奖阶段。演习结束后，红方和白方将协作提交一份演习行动报告书，描述每一个参赛队的网络防御情况，内容包括发生异常时冗余系统的可用性，蓝队提交报告的准确性等。白方将各队计分结果提交演习指挥部，分数最高的参赛队将获得国家安全局颁发的优胜奖杯，并保持到下一届演习。

此外，各方经过讨论后提交一份演习建议书，对整个演习的经验教训进行总结，为下一届演习提供参考。

## 5. 演习评估方法

演习评分标准基于各参赛队对服务功能的维护、对网络入侵的防御，以及对所有可疑行为的分析报告 3 个方面的表现。白方实时评估演习当中蓝队网络被破坏的服务、被攻陷的主机和其他发生的恶意行为，并实施罚分。每队初始分数为 50 000 分，红队成功的攻击将造成蓝队被罚分。另外，白方还根据某些科目的完成情况给予蓝队奖励分数。例如，对两台预配置服务器的漏洞进行正确分析，最高可获得 500 分的奖励分，对可疑个人计算机的取证分析以及 Web 服务器的灾难恢复也可以获得奖励分数。

网络防御演习的参赛军校队基本上由本科生组队。研究生参赛队给予同样计分，但不参与奖杯的角逐。表 2-2 为 2006 年网络防御演习参赛各队的得分情况，由于美国空军技术学院研究生队不参与奖杯角逐，奖杯由美国空军军官学校夺得。

表 2-2 2006 年网络防御演习参赛各队得分情况

参 赛 学 校	分 数	参 赛 学 校	分 数	参 赛 学 校	分 数
美国空军技术学院	50 550	美国西点军校	46 600	美国海岸警卫学院	44 100
美国空军军官学校	48 425	美国海军军官学校	45 650	美国商船学院	43 725

空军技术学院扮演蓝队，在经过红队 4 天的攻击后，其网络安然无恙，只出现了几处小的破绽。在演习过程中，该队发现，其中一台 Windows XP 工作站被国家安全局预置了恶意代码，不断设法与红队建立秘密连接。因此，蓝队决定对这台工作站进行系统还原。不幸的是，这台机器被安装了木马病毒，蓝队无法再信任其系统文件。这给蓝队带来了难题：系统不可用，必须加以还原，但系统还原会重新激活木马病毒。最后，蓝队还是决定实施还原，但机器中的某个恶意软件与红队建立了连接，几分钟后，蓝队才检测到恶意数据流并杀死进程。这次失误使美国空军技术学院队被罚分，但该队仍脱颖而出，赢得演习最高评分。

## 6. 2010 年网络防御演习

第 10 届网络防御演习于 2010 年 4 月 20—23 日举行，演习主题为“在敌对网络环境中的生存策略”。其含义是，设置复杂不可信的网络环境，限制蓝队可用的防御资源，使蓝队难以彻底驱除红队的攻击，蓝队需要采取的策略是：精心设计网络架构和事件响应方法，尽力抑制和缓和红队的攻击，保护关键系统和服务的正常运行和安全。

2010 年网络防御演习有 8 支军事院校队伍参赛，分别是美国空军军官学校、美国海岸警卫学院、美国商船学院、美国海军军官学校、美国西点军校、美国海军研究生学院、美国空军技术学院和加拿大皇家军事学院。

美国海军军官学校最终在 2010 年网络防御演习中胜出，赢得竞赛奖杯。

在 2010 年网络防御演习当中，红队由来自美国国家安全局、美国陆军预备役信息作战司令部、美国海军预备役信息作战司令部、美国空军技术学院、美国海军研究生学院、



加拿大武装部队信息作战大队、加拿大通信安全局、美国海军研究生学院的专家组成，大约 40 人，在国家安全局技术专家和往届有经验的红方工作人员的带领下对蓝方网络展开攻击。

白队大约有 20 人，约一半驻扎在马里兰州格林贝尔特 2010 年网络防御演习指挥中心，另一半作为一线裁判派遣至参赛军校。

2010 年网络防御演习要求蓝队网络提供的服务包括域名服务、Windows 活动目录、电子邮件、Web 服务、即时消息服务、文件共享服务、网络打印机服务、IP 电话服务。其中，IP 电话服务是这次新引入的服务内容。

2010 年网络防御演习的一个创新是加入了“灰方”，大约由 12 人组成，多数部署在参演军校。灰方人员充当蓝方网络的用户，在整个演习过程中进行邮件收发，创建、编辑文档，浏览网页，使用即时消息服务系统等。灰方所起的作用是：

(1) 在演习网络中产生正常的联网通信业务，避免蓝队人为假设他们所监控到的任何通信业务都一定是红队发动的恶意攻击。

(2) 扮演没有什么专业网络知识的用户，容易犯错，从而危害网络安全、给敌人的攻击提供可乘之机。

(3) 为演习营造动态的场景和虚拟化的事件，增加蓝队防御的难度。

在 2010 年网络防御演习过程中，白队临时插入了以下一些演习科目：

(1) 给蓝队网络临时添加工作站，其中一些工作站可能发现了恶意软件或其他安全漏洞。

(2) 在模拟的互联网上出现了明显带有敌意的“Web 爬豆”，蓝队无法对其进行阻塞，而必须对其进行处理应付。

(3) 对可疑计算机进行取证分析。

2010 年网络防御演习的另一个创新是“反攻”。35 家安全局在网络防御演习总部架设了一个目标网络，作为“靶场”供红队放手试验各种攻击技术，而无须像攻击蓝队网络时缩手缩脚。演习快要结束时，所有蓝队也被邀请对这个网络靶场开展攻击，进行了持续几小时的“擎旗”行动。在擎旗行动中，军校学员尝试获取代表着控制权的标志文件。这种靶场攻击和反攻行动可能被集成到未来的网络防御演习当中。

连续 11 届网络防御演习，充分体现美军对网络空间安全威胁的深刻认识、注重通过实战演练培养网络人才、积累网络攻防经验、加强危机应变能力。

### 2.8.3 “网络闪电”演习

2010 年 10 月 15 日，美国巴克利空军基地第 460 太空联队在周密计划的、竞争逐步升级的网络环境下，完成了独立的聚焦网络的演习。

## 1. 演习背景简介

此次演习名为“网络闪电”演习，旨在测试第 460 太空联队在竞争性网络环境中的运行能力。

8 名主题任务专家协助设计并实施了这次演习，他们均来自联队以外：第 688 信息运行联队、堪萨斯州空中国民警卫队（二者都属于第 24 空军部队）、网络运行与安全中心、埃利斯空军基地的前“网络攻击者”。专家们还帮助联队的演习评估小组评估了联队的表现，并总结了经验。请来的专家负责实施和评估整个美国空军的网络运行。这不仅仅是一次演习或比赛。它是一次实战，能大体了解在敌人试图破坏关键通信能力时，应如何指挥和控制基地，维护任务运行。

## 2. 演习过程简介

此次演习聚焦于：（1）网络降级、中断，以及黑客活动；（2）网络钓鱼和社会工程攻击试图访问空军基地网络和联队关键信息清单中的征询信息；（3）间歇性的陆上移动无线电、邮件弹出，以及聊天室能力，同时应对主动射手情景，反恐介入。演习还添加了“垃圾搜寻”功能，搜索未被正确销毁的个人或组织信息，一个办公室接着一个办公室地查询计算机中未被留意的通用存取卡，这种卡片能够授权对手访问联队网络。

一位参加演习人员描述道：网络进攻者侵入我的办公室，试图在计算机上注册，我注意到了限制信息，这种情况非常可疑。于是利用网络感知并阻止他们从任何地方接近我们的计算机。联队中有其他成员接到了攻击者打来的社会工程攻击电话，宣称他们是联队部署小组成员，诱使联队人员透露演习部署活动的信息，以及联队其他关键信息。

联队的政策规定：任何干扰全面网络演习的成员（成为“网络钓鱼”的牺牲品，或在没有“数字签名”的情况下打开电子邮件的链接），都会自动被锁定下线至少 24 小时，恢复网络访问之前必须接受网络安全程序再教育。

## 3. 演习情况总结

在演习中，第 460 太空联队的官兵有效地发现了各种网络攻击，并采取适当的防御措施，及时向上级和负责作战保密的小队报告。整个联队经受了正常通信工具遭到攻击或中断，依靠备用通信手段，保持了对部队的指挥和控制。

“网络闪电”演习完成了联队太空中队下达的目标：在所有常规通信手段和流程失效的情况下，确保继续指挥控制联队。美国空军将把网络空间战演习科目推广到空军所有联队的标准演习项目当中。

### 2.8.4 “施里弗”太空演习

“施里弗”太空演习是美军太空作战研讨会性质的模拟演习，核心目的是谋求太空优势。该演习 2001 年首次举行，之后大致每两年举行一次，为期 4 天到 8 天。截至 2016 年

年底,演习已进行了10次。演习由美国空军航天司令部航天创新与发展中心负责组织实施,演习主要围绕太空态势感知、太空部队增强、太空支援、太空控制和太空力量运用五大任务领域展开。战略意图是:通过构建有效的太空威慑,以太空优势谋求太空霸权;检验太空武器系统战技性能,提升太空和网络攻防能力;促进太空战略战术研究,辅助美国太空政策和战略制定。主要特点是:演习背景设定因时因势而变,注重航天新技术新装备的战法演练,拓展演习空间参演对象,强调盟国参与联合作战,太空战演习与理论创新同步互动。演习结论直接进入决策层,对美国制定和调整太空政策与太空战略,促进太空力量建设具有重要影响。

2010年5月7日至5月27日,美空军太空司令部打破以往两年组织1次演习的惯例,在内华达州的内里斯空军基地,进行了第6次“施里弗”太空演习。前5次“施里弗”太空演习分别在2001年、2003年、2005年、2007年、2009年举行。

“施里弗6”太空演习的假想作战时间设在2022年,但具体科目和前5次一样,保持高度机密。具体场景是在西太平洋阻止美国“势均力敌”的“对手”,对美国的太空与网络空间系统进行毁灭性打击。本次演习的目的包括:

- (1) 研究太空空间和网络空间的“替代概念、能力和力量态势”,以应对未来需求;
- (2) 探索太空空间和网络空间对未来威慑战略的贡献;
- (3) 探寻一体化的规划程序,以举国之力,保护并实施太空与赛博空间领域的运行。

演习关注的重点仍是太空和网络空间的作战问题,强调在未来全球冲突背景下的太空规划与威慑,突出了网络作战与太空一体化在支持国防方面的重要性,以及美国盟军、商业领域在太空及网络电磁空间能力方面的关键作用。

此次演习由美国空军太空司令部下属的“太空创新与发展中心”承办,美国军方和政府30个机构以及澳大利亚、加拿大和英国的550名专家,参加了此次为期20天的演习。这个“太空创新与发展中心”的前身是“太空作战中心”,主要任务就是通过创新、整合、训练测试和试验,来推动太空力量对全频谱作战(包括进攻、防御、稳定、支援在内的战争及非战争军事行动的统称)的支持。参与本次军演的机构包括:空军太空司令部、陆军太空与导弹防御司令部、海军网络与太空运行司令部、国家侦察办公室、国家安全太空办公室、空军作战司令部、国防部部长办公室、美国联合部队司令部、美国欧洲司令部、美国太平洋司令部、美国战略司令部、美国南方司令部、美国运输司令部、美国特种作战司令部、美国北方司令部、北美防空联合司令部(美/加)、国防信息系统局、国家地理空间情报局、国家安全局、国家航空航天局、国土安全办公室、运输部、国务院、商务部。

### 2.8.5 “网络卫士”演习

#### 1. “网络卫士”演习的历史

“网络卫士”演习从2012年开始。每年举行1次,至2016年已举行了5次。下面简

要介绍前 3 次的演习。

2012 年度“网络卫士”演习（Cyber Guard 12-1）的目的是促进联邦政府和州政府之间协调响应网络事件，探索利用国民警卫队的潜力作为网络空间域的附能者和“力量倍增器”。

2013 年度“网络卫士”演习（Cyber Guard 13-1）扩大了演习范围，作为一个协作性的战术级演习，重点是国家和州的防御性网络空间作战。国土安全部国家网络安全和通信集成中心、联邦调查局都参与了。

2014 年度“网络卫士”演习（Cyber Guard 14-1）提高了真实感，要求团队把信息报告给演习网络之外的州政府和联邦政府的网络中心。6 个州联合行动中心、国土安全部国家网络安全和通信集成中心监视部门与联邦调查局域网络特遣队、国家网络情报联合特遣部队（NCIJTF）积极参与了整个演习。

## 2. 2015 年度美国“网络卫士”演习

### 1) 简介

2015 年 6 月 8 日到 26 日，在弗吉尼亚萨福克最先进的设施中举办了 2015 年度“网络卫士”演习。动手操作的指令和演习场景在一个机密的封闭网络环境中进行，这个环境模拟国防部的和非国防部的网络。一个现场专家假想敌部队扮演各样的对手破坏美国关键基础设施。蓝军和友军努力保护关键基础设施网络并对一系列事件做出反应。

### 2) 参演单位

来自 100 多个机构（涵盖政府部门、学术界、产业界和盟友）的网络空间和关键基础设施操作员和专家参加了这次演习（第四届）。美国网络司令部、国土安全部和联邦调查局共同领导了这次演习。超过 1000 名参与者，其中包括陆军、海军、海军陆战队、空军的现役部队、海岸警卫队和预备役部队和人员，17 个网络保护分队和计算机网络防御服务分队人员，来自 16 个州的国民警卫队、12 个州的联合行动中心/紧急行动中心/融合中心和情报界的代表，来自三家私营行业信息共享和分析中心、第一个信息共享和分析机构（代表 16 个关键基础设施部门中的 8 个）、金融和能源部门的私人行业合作伙伴，还有国家网络安全和通信集成中心，基础设施保护办公室的人员。

### 3) 演习的目的

“网络卫士”演习的目的是：

- （1）提高部队保卫美国国防部信息网络及其数据，并缓解国防部的任务面临的风险。
- （2）支持国防部做好使命准备，保卫美国本土和切身利益免遭产生重大后果的干扰性或破坏性网络攻击。
- （3）提高政府机构、私营部门和盟国合作伙伴之间共享态势感知的能力。
- （4）改进功能和流程，以快速检测和有效应对影响美国关键基础设施的干扰性/破坏性网络攻击，这需要国家整体协调和努力。

(5) 加强政府、盟国和私营部门的伙伴关系。这种伙伴关系对于威慑和响应共同的威胁而言是至关重要的。

(6) 建立和维持国防部内部进行网络空间作战的战备和能力。在演习中,美国网络司令部评估网络任务部队各分队的能力和战备情况。

(7) 继续努力在国防部中为网络空间力量建设一个持久性的训练环境。这种持续性训练环境包括一个封闭的演习网络、训练活动规划、管理和评估、现场专家假想敌部队和保障分布式参与的传输层。其他美国政府部门、盟国和其他伙伴可以使用这种持续的训练环境,为全国性的网络空间作战训练奠定基础。

#### 4) 演习的阶段划分

第1阶段:按照国家应急响应框架和国防部对民事当局的防务支持,联邦和州政府支持私人部门、市政联邦政府和州所属的重要基础设施/关键资源。

第2阶段:为联邦机构提供防御支持,包括美国联邦航空管理局。

第3阶段:有针对性地训练国防部的网络部队和联合网络总部的人员,并提供认证。

经过19天的演习,参加者演练了如何对美国关键基础设施的破坏性网络攻击做出整体协调一致的响应。他们组成14个团队,承担不同的工作角色,提供训练、援助、建议给关键基础设施中常见的工业控制系统的私营企业和国防部任务的所有者,提高了美国网络司令部评估网络任务部队的能力和战备状态,表明了网络安全的准备和应对方法从“政府整体一致”转变为“国家整体一致”。

### 3. 2016年度美“网络卫士”演习

#### 1) 美2016“网络卫士”演习简介

2016年6月10日至18日,美国在弗吉尼亚州萨福克的联合参谋机构组织了2016“网络卫士”演习。这次是“网络卫士”演习的第5届。共有来自全美100个国家政府机构和私营企业的约800名参与者参加。联合参谋机构为演习参与者提供专用网络而不影响运作的网络。演习占据约48000平方米的可重构空间,超过1150个工作站,规划和工程耗时10~12个月。在演习控制室中心,如果参与者发现演习太过简单,规划者可以拨打对手电话要求提升能力;如果参与者发现演习太难,可以回拨。团队有必须实现的特定目标,在演习控制室的人员确保对手能让这些团队实现目标。

#### 2) 演习单位和合作伙伴

2016“网络卫士”演习由美国网络司令部、国土安全部和美国联邦调查局联合主办,其他参与者包括北方司令部、11个州的13个机构,主要包括国民警卫队、联邦航空管理局、国家合作伙伴(如英国、加拿大、澳大利亚)、行业合作伙伴、互联网服务供应商、电力公司以及港务局等,旨在检测国家在面临网络危机时的全面防御能力。

### 3) 演习场景和要解决的问题

该演习场景为：模拟美东北部轮流停电；模拟攻击海湾石油和燃气设施导致漏油；模拟攻击使加州海湾三大港口的装载顾客及商品船只和集装箱船只，使其陷入停顿等。2016“网络卫士”演习集中解决三大问题：国防部如何更好地保障其网络的安全；国防部及政府如何更好地防止重要基础设施遭遇毁灭性攻击事件；国防部在遭受攻击时如何为民间机构提供支持。

### 4) 美 2016 “网络卫士”演习特点

(1) 演习规模及参演人员素质大幅提升。此次演习无论从规模、涉及领域到人员数量都有所增加。四年前的第一届演习，参演人员主要为士兵、海员、飞行员和海军陆战队人员，主要体现在个人技能运用于训练，缺乏团队的整体作业。四年后，参演的是训练有素、整装待发的高水准团队。

(2) 演习各部门间合作关系更坚实紧密。国防部通过前四届演习不仅与其他联邦机构，还与私人企业建立了坚实的合作关系，因为美国私营企业是美国基础设施的重要组成部分。美军强调，有必要在紧急情况下与行业建立信任和合作关系。例如，有些组织虽然能力强，但却没有足够的资源或人力响应突发事件，需要其他部门给予支援。

(3) 演习训练环境适应性更强。美国联合部队发展部副部长表示，“我们正在构建实实在在的网络训练环境”。联合参谋机构为演习训练者提供了专用的网络环境。

### 5) 启示

(1) “一石二鸟”：美国通过演习达成网络部队建设目标。此次演习是检验美国在遭遇危机或紧急突发事件时，国防部将有能力和途径把网络资源借予民间机构，而且这是加强组建网络部队的关键步骤之一。美网络部队建设目标即截至 2018 年达到 133 支。网络司令部自 2009 年创立以来面临的挑战就是一边作战一边构建部队。据网络保护分队某成员透露，整个网络保护分队包含部队和地方人员共 39 人，根据每个人的技术能力承担不同的角色和任务。一旦整个网络部队部署完整，133 支网络部队中将有 68 支网络保护小组共同防御国防部网络。

(2) “立竿见影”：美以使命任务为牵引快速推进网络空间防御能力发展。国防部在网络空间的三大使命，即运行并防御国防部网络、准备防御美国重要基础设施和支持完成联合部队指挥官的目标。2016“网络卫士”演习目标主要集中在国防部的前两个空间使命。从美前四届演习来看，紧贴实际以模拟实战场景的训练模式效果很明显。美国网络国家任务部队司令称：“我们需要让团队一年内多次快速地执行这样的任务，通过演习，可以促进与合作伙伴之间的配合，我们需要通过演习来提高我们的网络备战能力。”

(3) “相得益彰”：美通过演习提高网络空间联合作战实际运用。在“网络卫士”演习期间，美国另一网络演习“网旗”也在同台竞技，并与“网络卫士”相配合。这两个演习在实现国防部任务使命上是一个整体，并且互为影响、互为促进、互为补充、不可分割。通过此举，可快速推进美网络空间联合作战能力的整体提升。

## 2.8.6 美军其他网络空间作战演习

### 1. 美国空军“防御壁垒”演习

“防御壁垒”演习是由美国空军主办、所有军种参加的一个全球性的年度网络防御演习。

得克萨斯州拉克兰空军基地的空军信息作战中心于2000年创立了“黑色撒旦”演习，以测试空军网络的防御能力。对于很多人来说，“黑色撒旦”演习就等同于在计算机网络上实施的“红旗”演习。参加演习的人员保卫关键的指挥和控制节点，抵抗来自第57和第177“信息侵略者”中队、第92信息战中队和国家安全局经过训练的假想敌人的持续攻击。到了2006年，这项演习被重新命名为“防御壁垒”，并扩大演习范围，陆军、海军和海军陆战队加入，以计算机网络防御为重点。

“防御壁垒”演习为各军兵种在网络空间领域开展联合作战提供了一块最佳的试验田，但演习没有包含电子战和心理战等信息作战的内容，也没有提供能把网络空间效应与由空基或天基装备所产生的效应整合起来的环境。

### 2. “虚拟旗”演习

2007年7月，美国空军举行了为期10天的“虚拟旗”演习，分布于世界各地的美国航空兵利用计算机网络虚拟的模拟器进行空战演习，以检验美军空战下的网络协同能力。F-16战斗机、A-10C攻击机、RC-135“铆钉”电子侦察飞机、E-8“联合监视与目标攻击雷达系统”，以及E-3“空中预警与控制系统”等飞机模拟器均在演习中投入使用。除了空军，海军“宙斯盾”导弹系统和陆军“爱国者”导弹系统也在训练中被模拟。值得关注的是，此次演习还首次引入了网络作战，参加者利用虚拟美军网络战部队，进行国家能力探测，以促成空战行动的顺利完成。

### 3. “网络拂晓”演习

2009年11月，美国国防部举行了名为“网络拂晓”的模拟网络空间战演习，通过对虚拟社会网的攻击与防御检验了美军网络空间战的技术水平。

#### 1) 模拟网络战

在弗吉尼亚州郊外，一座用夹板搭建的模拟军事指挥所旁，20多人聚集在一起，一人一台笔记本电脑，忙碌地操作着。他们看上去和普通人无异，有的身着整洁的衬衫、西裤，好似中年会计师；有的穿着彪马牌运动衫，头戴棒球帽；但他们却是一群职业黑客，担当此次“网络拂晓”演习中的进攻方。作为进攻方，他们的任务是利用一切不导致人身伤害的手段，入侵一个有一万名假想居民的虚拟网络，切断通信联络、修改社会保险账号，破坏电网，使城市应急系统陷于瘫痪。

他们的对手——“网络拂晓”演习的防守方，在不远处严阵以待。他们由10支队伍

组成，分别来自美国军方、军事学院（如美国西点军校、美国空军学院等）和民间安全防护公司，甚至包括一些未成年的电脑奇才。他们的任务是保护虚拟网络不受黑客袭击。

“网络拂晓”演习为期两天，对各种信息技术和网络手段进行了检验。

## 2) 攻击手段

通信系统和计算机网络是网络空间战中最易受攻击的目标，黑客的攻击手段也是层出不穷。在“网络拂晓”演习中，进攻方侵入防守方的操作系统，运行事先编好的攻击程序，他们还可以进入对方的系统，屏幕截图上面清晰显示了对方在计算机上的操作步骤，而对方却并不知道自已已受到监视。另外，攻击方的其他攻击手段还包括直接侵入敌方指挥官的电子心脏起搏器，使之无法正常工作。这种手段如同狙击手发射子弹一样精准，黑客们称之为“电子狙击”。

黑客还可以侵入敌国的银行系统，修改或删除账户，导致敌国政府失去信任，引发社会动荡。而远程侵入网络或使基础设施瘫痪的攻击方式则更安全、更便宜，人们不必冒着生命危险去偷文件，飞行员也不必顶着防空炮火去炸毁发电厂。

## 3) 攻防技术

在许多网络攻击案例中，隔离似乎是唯一的应对手段。在发动网络攻击方面，美国政府也是谨慎行事。因为即使现在有能力发动攻击，但却没有把握抵抗对方的反击，因为无法准确地定位攻击源。网络攻击从源头至目标一般经由他国网络，定位攻击源十分困难。

在“网络拂晓”演习中，防守方通常以牺牲某些领域的安全来守卫其他领域，可谓“壮士断腕”。“网络拂晓”进攻打响一小时后，美国空军学院竭尽全力保护电话通信系统。但是，在几分钟后，通信网络便落入黑客之手。

## 4. “网络冲击波”演习

2010年2月17日，美国举行了代号为“网络冲击波”的演习，该演习是由位于华盛顿特区的智库毕帕提森政策中心组织的。其目的是要让公众真切地看到当国家遭受网络攻击时，美国政府高官应对网络攻击的策略。此次演习的目的不是制造一场毫无实际意义的网络空间战争，而是用极具真实性的事件反映出相关政策的缺失。政策中心组织在首都华盛顿的一家宾馆里设置了虚拟的“紧急情况处理中心”，并将多名前任白宫官员及前任国家安全官员集中在那里。此前，他们并未被告知本次演习的性质和内容。根据设定，在长达3小时的演习过程中，美国的手机通信网络首先遭到破坏，黑客们随后将利用智能化技术中存在的漏洞对国家供电系统展开攻击。起初，攻击的性质类似于有组织的犯罪行为，但随着事态的不断升级，国防部将介入此事，并对是否进行反击以及反击的方式做出决断。

## 5. “锁定盾牌”网络空间作战攻防演习

“2013 锁定盾牌”网络攻防演习，于2013年4月24日至25日在北约合作网络防御卓越中心举行，是美国、北约和诸多西方国家联合组织、联合参与、联合实施的一种“非传



统军事演习”，同时也是它们在占领网络空间的战役中举行的一次“实战演习”，主要检验北约快速反应部队的协同作战能力。虽然在组织形式、兵力投入等方面与常规军演有明显区别，但参演双方开展网络攻防对抗的激烈程度和相似程度远高于常规演习。针对日渐严峻的网络安全问题，通过制定网络立法、开展网络演习和组建网军部队等措施，实施对网络空间的绝对控制。


这是一场红、蓝军攻防演习，参演的数十个蓝军部队需要保卫自身的网络不受网络攻击；这是一场国际性的演习，来自 15 个不同国家的 18 个组织参与并准备演习，思科、Bytelife、Clarified Networks 等世界重量级计算机基础设施公司为其提供技术支持。演习的类型属于游戏性质，参与的各小组并不代表它们的组织和工作，所有角色都是虚拟的。演习在一个实验室环境下进行。蓝军是主要参演对象，他们需要保护一个预先建立好的、含有漏洞的网络。为了评估不同的战略和战术，将对蓝军进行自动化和手动的评分。每组蓝军都会配备 1~2 名法律顾问。红军的任务主要是入侵或干扰蓝军手中的系统。红军预先知道蓝军手中系统的漏洞，并且在演习开始之前，红军可以扫描蓝军网络的漏洞。白军负责整个演习的组织工作。他们制定演习目的、场景，与红军一起开展攻击活动、编写规则。绿军负责准备演习的技术设备。黄军负责搜集、分析演习的信息，并向控制室传递最新的演习情况。

## 6. 美陆军“网络闪电战”演习

2016 年 4 月，美国陆军第 25 机步师和第 7 信号指挥网络防护旅举行了“网络闪电战”演习，演习地点是美国陆军装备司令部通信—电子研究、开发与工程中心。演习的重点是在逼真的训练场景下测试新型作战概念，解决网络电磁行动的交互问题。士兵们通过一系列仿真场景将通信、网络防护、电子战和频谱分析等纳入战术作战中心的职能进行演练，检验了主要指挥所的物理构造以及各军事作战专业之间的交互，以使网络、情报、电子战连通并更好地融合；然后通过无缝单元协同工作，就能够交换数据并明确任务威胁的方位，以及如何做出更加明智的决策。

“网络闪电战”演习所取得的成果，不仅有助于美国陆军战术作战中心制定相关条令，如何支援前方作战旅的网络作战行动，还有助于美国陆军做出更好的投资决策。





# 第 3 章

## 网络空间作战武器

网络空间作战武器是夺取信息优势的关键装备，是提高武器整体作战效能的倍增器，是诸军兵种实施联合作战的“纽带”，是武器体系中发展最快、最不可缺少的重要内容，是获取“制网络权”的基础。网络空间作战武器渗透性强、数量多、门类杂、规模大小不一，为了在其研制上取得重大突破，各国都在加大投入，加速网络空间攻防武器的研发力度。确实，要想占领现代战争制高点，就需要对网络空间作战武器有一个全面、正确的认识与把握。

### 3.1 网络空间作战武器基本内容

#### ■ 3.1.1 概念与特征

##### 1. 基本概念

网络空间作战武器泛指所有工作在互联网、无线网以及各类局域网中能够对战争产生影响的所有软硬件，或由硬软件组成的系统，或者基于网络的设施和平台；既包括人们所

熟知的各类病毒、木马，也包括一些功能正常的网络应用，还包括元器件以及可以接入网络的各类设备。这是专门用于突破敌方网络系统、安全防范体系的特殊武器，能对敌方军用系统或与之相关的民用系统、信息系统等进行侦察、侵扰、欺骗和破坏，使其信息处理效能、网络通信作用、武器作战能力等降低或丧失，并能有效保护己方网络与信息系统免遭敌方攻击。具体表现为：在网络环境下，以网络信息技术为主，具有信息产生、获取、传输、处理、应用等独立功能，可摧毁、破坏和瘫痪敌方网络系统，阻止敌方战场信息的获取、传递、处理和应用，使敌方丧失指挥控制能力。

## 2. 本质特征

由以上的概念可以看出，网络空间作战武器有以下几个本质特征：

(1) 网络空间作战武器的使用环境是网络环境，战场要素包括计算机应用系统、网络通信系统和网络平台等各种软、硬件系统；其作战系统可能依托陆、海、空、天战场，但它并不是对上述战场的争夺。

(2) 网络空间作战武器的使用目的是夺取制网络权，目标在于攻击敌方计算机网络系统，阻止敌方战场信息的获取、传递、处理和应用，使敌方丧失指挥控制能力，同时保护己方战场信息流程通畅。

(3) 网络空间作战武器的对抗使用的是非常规手段和弹药，以信息伤害为主要攻击手段。通过扰乱、破坏和瘫痪等方式，使敌方掌握的信息失去完整性、真实性、准确性、可用性和实时性，从而无法实施及时有效的指挥。

(4) 网络空间作战武器的核心技术是以计算机和网络技术为主的信息技术。

(5) 网络空间作战武器具有无形性、隐蔽性和可控性。

① 无形性是针对武器的存在形态而言的，武器中最重要的表现形式——杀伤手段由传统的硬火力变成了软信息。

② 隐蔽性是针对武器的攻击行为而言的，网络空间作战武器使用无形攻击手段去封锁敌信息来源、切断敌信息传输、破坏敌真实信息、瘫痪敌信息系统、示敌于虚假信息，一切都在悄无声息中进行。这种极强的隐蔽性，使对这种武器的防范更难，甚至可以毁敌于无形之中，而敌无从觉察，无处躲藏。

③ 可控性是针对武器的攻击效果而言的，常规武器一旦实施攻击，其打击效果是不可控制的，使用时机和投送方式受一定条件制约，杀伤范围也是有限的。而网络空间作战武器的运用却不受这些条件的限制，可以在平时进行，也可以在战时进行，在攻击的时间、地点、目标和方式选择上都有极大的灵活性。

### 3.1.2 主要对象、任务和目标

网络空间作战武器是人类向信息社会转型过程中出现的新生事物，主要对象是信息基

基础设施；主要任务是实施管控；根本目标是体系击破；本质上体现了安全观念、战争观念和作战理念的变化；已经激励了全球国防科技的创新发展热潮。

网络空间作战武器的主要对象是军用和民用信息基础设施。它针对物理域、信息域、认知域、社会域内的不同应用要求，按照不同的对抗形式和效果，选择不同的发展重点。在物理域，网络空间作战武器发展以电磁对抗武器为主，针对时间、空间、频率、能量、调制等方面的对抗，包括发展应用于陆、海、空、天的各类电子侦察、电子进攻、电子防御、特种电子对抗和新概念电子对抗武器，其本身也正在向全谱化、综合一体化发展，向多样化、精确化、隐身化、无人化、高效化发展。在信息域，网络空间作战武器以网络信息对抗武器为主，包含物理层、协议层、信息层、行为层攻击与防御手段。在认知域，网络空间作战武器以智能对抗武器为主，包含协同、欺骗、控制手段，其重要的特征是控制人们的感受、情绪、意识和理解；在社会域，网络空间作战武器以泛在对抗武器为主，包含多种方式综合运用和体系击破等方式，将通过多种方式进行体系对抗攻击。

网络空间作战武器的主要任务是实施管控。无论早期网络空间作战武器、高级网络空间作战武器，还是正在快速发展的网络空间作战武器体系、网络作战基础设施等，网络武器发展的主要任务，都是以增强“控制”能力为核心，对敌方军用和民用信息基础设施实施管控。目前，网络空间作战武器不仅在手段上呈现了层次化、融合化的趋势，在控制上呈现了协同化、智能化的趋势，在应用上呈现了多样化、泛在化的趋势，而且对武器体系研发与集成提出了新的要求，为部队训练与作战提供了新的有效手段，已经引起“非接触作战”“软杀伤”等作战概念得到进一步发展，已经引发了武器体系格局的变革。

网络空间作战武器的根本目标是体系击破。包括实施网络侦察预警、攻击、防御与作战支援的一系列武器，作为进行网络空间对抗的工具或平台，是夺取网络作战优势的关键因素，是保卫国家网络安全的制胜力量。尽管不同领域内网络武器的发展重点不同，但是网络武器发展的根本目标都是体系击破。它继承了信息化武器体系向协同化、智能化、多样化、泛在化方向的发展趋势。

### 3.1.3 网络空间作战武器的能力体系

要想在计算机网络战中获取网络信息优势，网络空间作战武器必须具备网络态势感知能力、网络进攻能力、网络防护能力和网络支援能力。

#### 1. 网络空间作战武器态势感知能力体系

网络空间作战武器态势感知能力体系包括：

信息获取能力：主要指对敌方信息的探测、监视、感知、录取、寄存和输入的能力。例如，网络攻击前的端口扫描、漏洞扫描、知识发现和数据挖掘等方面的能力。

态势要素获取能力：包括综合采取网络侦察、情报、技侦等技术手段，通过主动与

被动结合的方式获取网络空间的网络数据、环境数据和行为、内容数据等的能力。

**态势理解能力：**包括数据融合、目标识别、态势分析和信息内容分析等。数据融合主要完成对多个信息源的数据进行自动监测、关联、相关、目标聚类处理，从而得到更为准确、全面的信息；目标识别是在数据融合和处理的基础上，对目标进行初步分析；态势分析是将目标识别的结果归类为对手或己方，进行区别分析，进而综合形成当前安全态势；信息内容分析是通过对文本、图像和语音等信息内容进行关联分析，实现对意图、情报等的掌握。

**态势预测能力：**包括知识库、趋势预测、风险预测和态势推演等。

**信息处理能力：**主要指信息的传输、变换、校核、纠错、存储、显示、分析、输出和反馈的能力，如信息归并、信息格式转换和信息筛选等方面的能力。

## 2. 网络空间作战武器进攻能力体系

网络空间作战武器进攻能力体系主要包括以下方面。

(1) 入侵能力。采用直接或者间接方式，通过网络或其他设施入侵敌方网络、操作系统或应用系统的能力。

(2) 破坏能力。破坏敌方网络基础设施、操作系统、应用系统及其关键信息的能力。破坏能力可进一步划分为两个子能力：一是入侵敌方网络前的破坏能力，如消息阻塞、篡改的能力；二是入侵敌方网络之后的破坏能力，如计算机病毒的破坏能力。

(3) 欺骗能力。伪装攻击行为与攻击者身份，欺骗敌方网络监控系统，达到刺探情报、隐蔽入侵目的的能力。

(4) 窃取能力。窃取敌方保密信息，隐蔽传送的能力。

(5) 利用能力。利用第三方网络资源，实现分布式间接攻击的能力，比如分布式拒绝服务攻击的能力。

## 3. 网络空间作战武器防护能力体系

网络空间作战武器防护能力体系包括以下主要内容。

(1) 信息保密能力。保护敏感信息的存储、传输和利用，防止信息非法泄露的能力。

(2) 信息确认能力。严格限定信息的共享范围达到防止信息被非法伪造、篡改与假冒的能力。

(3) 网络控制能力。控制网络通信连接和安全管理的能力。

(4) 攻击检测能力。检测非法攻击行为的能力。

(5) 访问控制能力。控制用户访问受保护资源的能力。

(6) 隐藏欺骗能力。隐藏通信数据流、敏感信息或关键服务的能力。

(7) 响应恢复能力。响应入侵事件，遏制入侵行为，恢复被损系统和信息的能力。

(8) 免疫防护能力。抵抗已知攻击、弥补防护缺陷，增强防护策略的能力。

(9) 鉴别审计能力。鉴别实体身份、加强审计监督、防止身份冒充的能力。

(10) 病毒防治能力。防御、检测、清除计算机病毒和恶意程序的能力。

#### 4. 网络空间作战武器支援能力体系

网络空间作战武器支援能力体系包括以下主要内容。

(1) 决策支持能力。它主要指对获取信息进行决策分析,为指挥人员提供决策支持的能力。

(2) 信息通报能力。将作战信息通报给相应的作战部门,保障作战单元间的互通、互连、互操作和信息共享的能力。

(3) 网络通信保障能力。它包括网络通信的快速反应能力,高效快捷的协同能力,机动灵活的应对能力。

(4) 效能评估能力。评估网络攻防作战效能,发现未知缺陷的能力。

### 3.1.4 网络空间作战武器的分类

网络空间作战武器的分类标准和方法因学术理论观点、实战运用习惯和组织管理体系的不同,可以有多种不同的理解、认识和区分方法。这里,从作战运用、作战任务和作战中的表现形式三个方面对网络空间作战武器进行分类。

#### 1. 按作战运用分类

网络空间作战武器可以依照在作战运用上所处的地位与作用对其进行分类。根据武器的一般原理,有些可达成战略打击效果的武器属于战略级武器,而有些具有一般杀伤能力和较小杀伤范围的武器运用,则属于战术级武器。根据这一规律,考虑到网络空间作战武器与常规武器的作战共性,认为按照作战运用级别可将网络空间作战武器分为战略级网络空间作战武器、战役级网络空间作战武器、战术级网络空间作战武器和应急机动型网络空间作战武器。战略级网络空间作战武器是指那些可获得控制或瘫痪敌人整个指挥控制网络系统、能对战争全局起决定性作用的武器,如获得网络指挥控制中心根目录权限的黑客和具备全局感染、影响或瘫痪整个网络系统的病毒等;战役级网络空间作战武器是指可对某一大型作战区域起关键性胜负决定作用的武器,如防护某一战役级网络区域的防火墙等;战术级网络空间作战武器是指那些攻击与防护台站型武器的节点级网络空间作战武器;应急机动型网络空间作战武器是指那些在网络系统遭到大范围损伤的情况下能够继续运行并提供基础性、关键性服务的武器,如应急密码、密钥、机动性方案等。

在实际的作战使用中,这些武器是彼此融通,甚至可以相互转换,即有些武器在不同的作战环境与作战系统下,可能会表现出不同的作战效果,如某些应急机动型武器,在条

件充分的情况下也是可以达成战略级作战效果的，这也是网络空间作战武器区别于常规武器的一个重要方面。

## 2. 按作战任务分类

根据各种武器在网络空间作战中所体现的任务，可将网络空间作战武器划分为网络空间态势感知武器、网络空间进攻武器、网络空间防御武器与网络空间支援武器。

网络空间态势感知武器主要实现网络态势感知，侦察并分析目标运行状况和网络行为等动态信息，遂行己方、敌方以及其他相关行动信息的即时理解，对网络空间威胁进行预测和告警，为判别对手行动意图提供支持。如美国的“爱因斯坦”计划、安全管理引擎、主机入侵防御系统、流氓系统探测、装置控制模块/数据丢失防御、链路数据捕捉系统、传输/数据协议分析系统、情报分析系统等属于网络空间态势感知武器。

网络空间进攻武器是指利用敌方网络空间系统安全缺陷，为窃取、修改、伪造或破坏信息，以及降低、破坏网络空间使用效能而采取各种措施和行动的武器。主要包括计算机病毒、木马、逻辑炸弹、网络分析仪、探测软件、目标链路接入系统、信息平台攻击系统、协议/链路攻击系统、石墨炸弹、电磁脉冲弹、高能/定向能武器、微米/纳米机器人、担任攻击任务的智能网兵（即移动 Agent）和美军的舒特机载网络攻击系统等。在此分类中，还可进一步细化，如网络进攻武器可分为软杀伤和硬杀伤两类。软杀伤武器是指对敌方网络系统硬件不具有直接的杀伤、破坏和摧毁作用，但可对敌方网电系统中的信息、信息过程、信息系统和信息能力起干扰、破坏和控制作用的网络武器，主要包括各种病毒软件和网络攻击工具或软件等。硬杀伤武器是指对敌方网络系统硬件具有直接的杀伤、破坏和摧毁作用的网电武器，主要包括激光武器、电磁脉冲武器和电子生物武器等。

网络空间防御武器就是在网络空间作战中，为保护己方网络系统和设备正常发挥效能而采取措施和行动的武器。主要包括攻击检测、网络安全监控与告警、网络防火墙、入侵检测软件、网络防御软件、担任防御任务的智能网兵、数据加密、网络安全协议、病毒免疫卡、病毒检测与消除、审计跟踪、安全密钥管理等手段，其中加密设备和防火墙始终是网络防护的两大核心武器。比较有代表性的有美国空军“网络诱骗”系统、“网络狼”软件系统、深查威胁管理系统、深查告警服务系统、网络漏洞扫描仪、陆军入侵检测系统和空军抗太阳辐射型空间路由器。特别是美军的深查威胁管理系统，它可以对网络信息系统所面临的潜在威胁做出告警并推荐相应的反应手段。

网络空间支援武器是专门用于网络空间作战中各种支持活动的装备，主要为网络空间对抗及网络武器的开发、测试、评估、采办等方面提供支持和保障。例如，漏洞评估、基于威胁的安全评估和修复等。

这种划分方法符合传统战争基本特征即进攻与防御，而且便于与常规武器体系进行耦合。

## 3. 按作战中的表现形式分类

根据武器在网络空间作战中的表现形式，可将网络空间作战武器划分为网络空间作战



软武器和网络空间作战硬武器。像各种病毒软件、网络攻防工具或软件、网络操作系统、数据库、移动代理（Agent）等这些计算机系统的软件归为网络空间作战软武器；而像激光武器、电磁脉冲武器、电子生物武器、服务器与工作站、防火墙、网卡、路由器等这些计算机系统的硬件可归为网络空间作战硬武器。这种划分方法既体现了网络空间作战与计算机系统的特征，又便于对所有武器进行准确划分。

### 3.1.5 网络空间作战武器的作用

总体上，网络空间作战武器通过在战争准备、发动、初始、胶着、结束等各个阶段发挥作用，使得未来战争向可控方向发展。谁能充分发挥网络空间作战武器的控制作用，谁将赢得战争胜利。

#### 1. 在战争准备阶段搜集情报

通过利用网络空间作战武器搜集网络情报，并与其他来源的情报进行深度融合分析处理，可以获得一个国家政治、外交、军事、经济、科技等领域的全方位情报，进而对一个国家的政治局势、外交政策、军事力量、经济发展和科技研发等方面进行综合评估，增强国家之间的透明程度，利于在战争准备阶段进行战略预判和战略评估。在出现可能导致力量对比发生重大变化的因素之前就采取适当的措施进行干预，使对方始终处于劣势而无法摆脱受控局面。如果和平的措施无法达到干预效果，则在己方仍能稳操胜券、对方未能扭转被动局面的前提下发动战争，达到有效遏制对方行动的目的。

#### 2. 战争发动阶段宣传造势

一方面，通过在战争发动阶段宣传造势，积极获取国内外广泛支持，为顺利发起战争奠定道义基础，可有效防止其他国家干涉，对于控制战争规模和时间具有重要意义。例如，在利比亚冲突期间，社交媒体成为反对派与外部世界交流，特别是与各个国际媒体沟通的最有效途径之一，通过社交媒体宣传，获得了广泛支持。国内反对派组织以及国外流亡者的“推特”信息、“优兔”网站视频、“脸谱”网页以及互联网博客，成为世人得到事态发展信息和图像的主要来源，为联合国安理会顺利通过国际军事干预的决议提供了信息支撑。

另一方面，随着世界各国日益重视社交媒体的颠覆作用，政府对于互联网接入进行了适当控制，以防止恶意用户传递非法信息。针对这一情况，西方发达国家纷纷重视研究新型网络渗透技术，“动乱互联网”“手提箱互联网”等应运而生。利用“黑莓信使”“手提箱互联网”和“动乱互联网”等网络渗透工具，可有效避开他国网络管制、从事颠覆破坏活动。

由此可见，在一系列网络渗透技术和工具的支持下，战争发动方利用网络媒体传播敌

国腐败、失业、贫困等社会突出问题，丑化敌方政府，甚至散布虚假消息煽动民众情绪，激化社会矛盾，实现其扰乱社会正常秩序、制造纷争事端的目的，为出兵宣战、进行军事干预创造可控的动机，夺取道义上的主动权。

### 3. 战争初始阶段制敌控权

现代战争多以争夺制信息权、制空权为战争初始阶段首要目标。综观 20 世纪 90 年代以来的多场局部战争，无一不是首先瘫痪指挥控制网络和防空系统，为己方实施空袭提供安全通道。随着武器系统的信息化程度不断提高，随着国家关键基础设施的自动化程度不断提高，网络空间作战武器可在战争初始阶段有效瘫痪敌方武器系统和敌国的关键基础设施，进而实现制敌控权的目的。

一方面，武器系统的信息化程度不断提高，武器系统自身安全难以保证。经历了二十多年的发展，武器系统包含电子元器件，数量规模庞大，逻辑程序更加复杂，很难确保其安全性，这为安置网络空间作战武器提供了可能。通过在出售的电子元器件、指控程序等内部植入病毒，可使带有病毒的硬件或软件在其武器系统中长期潜伏，在日后发生军事冲突时激活，瞬间达到瘫痪敌方武器体系的目的。

另一方面，国家关键基础设施自动化程度不断提高，关键服务提供难以可靠保障。2010 年震网病毒以及 2012 年“火焰”“高斯”病毒的相继暴发告诫人们，工业控制系统存在着极大的安全隐患。可想而知，在战争打响之际，突然电力系统、水力系统瘫痪，既无法满足军事斗争需要，连社会稳定都无法保障，从而大幅度地动摇民心 and 战争斗志。

此外，社交媒体还可以用于重要目标指示，为进攻方提供可靠的目标信息。例如，在利比亚冲突中，一部普通的移动电话或卫星电话可以作为一个非常强大的前方空中引导控制工具，使用地理信息和地图绘制服务，生成经纬度数据并利用推特（是一个社交网络及微博客服务的网站，是全球互联网上访问量最大的十个网站之一）将目标图片及坐标传给北约，为联军攻击提供引导。

由此可见，网络空间作战武器通过预置、病毒感染等手段可以广泛渗透到电力、水力、金融等关键基础设施和武器系统，特别是指挥控制和防空网络中，并可通过社交媒体传递重要目标信息以供打击，这些都为战争发起方有效掌控战场形势奠定了坚实基础，从而在战争初始阶段就牢牢握住制胜基石。

### 4. 战争胶着阶段攻心扰敌

当战争进行到一定阶段，战争发动方已经在战争局势上占据完全主动，通过心理宣传、心理欺诈和心理威慑等心理战手段，可从精神上进一步瓦解敌方的抵抗意志，从而加速战争进程。网络空间已成为心理战的重要作用领域。

一方面，可以利用网络有效攻击敌方决策者的思想信念。在伊拉克战争中，美军故意保留伊拉克的网络设施，便于对伊拉克军政高官实施网上心理战。美军运用网络发布进攻信息，挑拨其与萨达姆的关系，通告高官被俘情况，甚至公然高价收买拉拢，使伊拉克高官处于人人自危的境地。

在多国部队空袭利比亚军事行动中,以美国为首的西方国家利用网络技术,向利比亚政府和军队高层实施了全方位、全时空、系统化的宣传、欺骗和干扰,通过发送电子邮件和手机短信瓦解利比亚政府军高层。

另一方面,利用网络欺诈手段削弱敌军士气。士气是战争过程中支配和影响军人行为的一种精神心理状态,是军人认识、情感和意志的综合体现,也是部队战斗力的重要组成部分。在伊拉克战争和利比亚冲突中,网络欺诈都起到了良好的心理战效果,达到扰乱民心、涣散斗志的目的。

由此可见,网络已经成为心理战的利器,广泛应用到战争进程中,通过电子邮件、手机短信、网络媒体等一系列手段影响改变敌方的心理状态,直击敌方官兵的精神世界,有效瓦解敌军的心理底线,使得敌方军队被打得摧枯拉朽般溃不成军。

### 5. 战争结束阶段社会重建

战争是政治活动的延伸。归根结底,战争是为了实现政治目的,因此战争结束并不代表政治活动的结束,胜利方会立足自身利益,采取政治、经济、军事、技术等一系列手段,对失败方进行重塑,以期达到长期控制。例如,在伊拉克战争后,美国希望将伊拉克建成政治民主化、经济自由化、社会世俗化的典范,塑造美国统治下的和平、民主国家。

网络时代的来临为战后重建提供了替代选项,一方面将先进信息技术输出到战败国可以提高战败国人民的生活水平和文明程度,加速社会信息化进程,增强战败国人民对信息技术的依赖;另一方面,可以在建设过程中预置后门,将网络空间作战武器广泛部署到各类关键基础设施中,实现战略预置,便于日后发难。

随着关键基础设施对网络的依赖性逐渐增强,网络空间作战武器必然被越来越多地用到战后重建的过程中,推广技术应用比推行民主制度具有更加明显的优势,同时也可以为日后更全面的控制奠定良好基础,达到对未来战争的控制。

### 3.1.6 网络空间作战武器的发展趋势

以目前的研究成果来看,现有的网络武器研究主要针对某项网络空间作战能力的增强,而忽略了武器整体作战效能的提升。未来,网络空间作战对网络武器整体作战效能的要求将会越来越高,需要在侦察到目标后能够迅速做出判断和决策,并实现对目标的识别、跟踪和打击等功能。因此,从实际应用的角度考虑,网络武器的发展方向是集侦察、识别、分析、接入、攻击、评估、决策等作战手段于一体,即新概念的一体化智能网络武器系统。

相比于单功能网络武器,一体化智能网络武器系统具备两大优势:一是可以实时地向所侦察并已确认的敌方目标进行网络打击,极大地提高作战效率,避免贻误战机;二是可以节省网络作战域内各节点之间的信息交换通道,提高作战隐蔽性,减轻己方信息网络的

负担，同时也降低了在网络作战中由于通信信道被破坏而失去战斗力的危险。智能网络武器系统的一体化作战主要包括 6 个连续的作战进程。

(1) 探测识别。对网络作战区域进行检查和探测，广泛收集各种军事信息并进行采集筛选，实施目标识别进而确认敌方。

(2) 目标扫描。对敌方的网络防御系统及周围的战场环境和态势进行自主动态认识，获取关键特性参数，确定敌方防御系统的结构特点及薄弱环节。

(3) 策略制定。根据所获得敌方以及战场环境的各种信息和参数，自主制定最优化的网络攻击策略（包括攻击范围、攻击方式、攻击流程等）。

(4) 主动接入。利用所获得敌方系统进程或安全措施中的缺陷或漏洞，在未授权的情况下接入到敌方的系统或网络之中，实现与敌方目标的互联。

(5) 攻击对抗。在进入攻击区域后，利用已制定好的攻击策略对敌方发动网络攻击，以实现干扰、控制、破坏敌方电子设备、计算机网络等设施的目的。

(6) 评估决策。对攻击后的作战效果进行评估，从而形成基于后续战场态势的判断与分析，及时修正网络攻击策略，对需要进一步攻击的敌方目标实施定点打击。

在上述作战进程中，一体化智能网络武器系统可随时将态势信息经由安全加密信道传送到友方作战单位或后方的指挥控制中心，以获得下一阶段的作战指令和任务。

因此，利用一体化智能网络武器系统，未来的网络空间作战将不再是启动就不管的工作状态，可以通过网络空间内敌方目标信息的收集、处理和传递，准确地感知态势、透视战场、锁定目标，快速地进行目标分析与全程决策，并且实时、高效地执行精确的网络打击，从而实现网络作战的智能化与一体化。值得说明的是，未来的网络空间作战样式很可能是一定数量的一体化智能网络武器系统联合作战，与指挥控制中心共同组成一个大型的、安全的分布式作战网络。这样，由于各个武器系统通过信息网络连成了一个整体，实现态势信息共享和作战的高效协同，将改变各个武器系统仅能在一定区域内作战，以及攻击样式有限等问题，以联成一体的网络作战网络为基础，以最佳的作战效果为目的，形成灵活多变的网络空间联合作战方式。

## 3.2 网络空间心理战武器

实施网络空间心理战，不仅需要专业的作战队伍，还需要特定的武器。在网络空间心理战中所使用的武器是心理战专业力量用于实施和保障战斗行动的武器、武器系统以及与之配套的其他军事技术武器的统称。它包括用以影响目标对象的心理及行动的各种战斗武器和实施技术与后期保障的各种保障武器。网络空间心理战武器是心理战所依托的物质基础和技术支撑，是形成战斗力、发挥政治工作作战功能的基础所在，其发展水平体现了一个国家在信息化时代的军事威力、经济实力和科学技术水平。

### 3.2.1 网络空间心理战的概念与特点

#### 1. 网络空间心理战的概念

根据中国军队《军语》所做的解释,心理战是运用心理学的原理,通过宣传等方式从精神上瓦解敌方军民的斗志,或清除敌方宣传所造成的影响的对抗活动。根据《心理战纲要》,心理战是根据战略意图和作战任务,运用特定信息和媒介,通过理性宣传、意志威慑和情感引导,对目标对象的心理及行动施加影响,促进政治、军事斗争目标实现的作战行动。心理战本质上是一种应用信息对目标心理施加影响的作战。传统的心理战主要运用于陆、海、空域,但随着网络空间域的形成,该域为心理战部队提供了新的作战进攻与防御领域。

所谓网络空间心理战,是指运用心理学原理,以网络空间为心理战信息传播载体,发布心理战信息,使敌方军队士气瓦解和敌方民众对当局不信任,同时鼓舞己方军队人员士气和己方民众进行教育,以达到支持己方军事行动进攻与信息防护的作战方式。在网络空间载体上发表的信息内容涉及一切与战争相关的社会、政治、经济、文化、人权、宗教信仰、种族矛盾、政要人物丑闻、军事实力对比等领域。采用传送虚假信息,误导预定人群,介入对方数字空间,不同程度地操纵媒体等,来达到干扰对方正常的社会秩序、军事准备、军事实施,使对方民众丧失对政府的信心以及动摇军心的目的。网络空间心理战是网络空间技术和心理战结合的产物。网络空间技术创新性、不稳定性、特殊边界性和高速性等特点必会促使网络空间心理战这一新型作战样式的产生与发展。

#### 2. 网络空间心理战的分类

网络空间心理战从不同角度可以划分为不同的类型。从战略层面看,网络空间心理战可以划分为政治、经济、军事、外交等几个方面;从战术层面看,网络空间心理战可以划分为心理宣传、心理威慑和心理欺骗等几个方面;从技术层面看,网络空间心理战可以划分为信息技术、多媒体技术、虚拟现实技术等几个方面;从作战样式看,网络空间心理战可以划分为网络心理进攻和网络心理防御。

#### 3. 网络空间心理战的特点

网络空间心理战将传统的心理战思想、心理学原理与网络空间技术,特别是网络信息技术相融合,具有以下鲜明特点:

(1) 作战领域宽广。作战领域可突破传统军事斗争界限,在军事、政治、经济、外交、文化、宗教等诸多领域进行全方位战略行动;而且可以应用于战争时期、准备期间、和平时期,贯穿于战争全过程,辐射到作战前沿、战略纵深、后方民众和国际社会等方面。

(2) 战术手段灵活多样。可以通过网络宣传、恫吓、欺骗、诱惑等手段,同时,随时根据受众反应进行调整,长期影响对方群体心理。另外,信息技术的发展使网络空间心理战的手段不断更新,信息媒介、投送手段、收集加工技术等向自动化、高速化、信息化方向发展。

(3) 信息传递实时性强、隐蔽性高。在网络上,信息以光速传播,即使相隔万里,一个地方发生事情,几乎另一个地方也能同时知晓;而且网上可以匿名发表言论,身份难以追查。

(4) 受众开放性强、交互性高。随着网络技术普及,人们接收信息更加便利,拥有更大的知情权和话语权。而且,心理战人员与受众之间交互性更强,新型媒体技术可使交互更隐蔽、更高效,使心理战作战周期缩短、作战节奏加快。

(5) 防御控制困难。网络防控一直是“道高一尺,魔高一丈”的态势,新型社交网络成为一种人们可以从众多地点互相联系的社交工具,无须访问主站点就能发布信息,致使防控极难实现。

(6) 整体威力增强。网络空间拓展了心理作战的空间,使心理战的威力空间具有真正的全球性;丰富了心理战的作战手段,尤其是在战略层面上威力明显增强;进一步增强了各领域心理战之间的统一性;提高了心理战的反应速度,因为网络空间具有很强的即时性、共享性和交互性。

(7) 非常灵活。网络空间力量的物理性暴力与心理性暴力将形成高度的统一,使心理战效应成倍增长。

(8) 平战界限模糊。网络空间心理战一个重要的趋势就是突破了所谓平时与战时的界限、前方与后方的界限、国界与地域的界限、战区与非战区的界限、敌我友中立的界限,随时随地都可能发生对抗,成为全时空、全地域的斗争形式。

(9) 军民难分彼此。网络空间心理战体现在军网与民网一体化,军用信息技术与民用信息技术一体化,网络心理战主体和客体多元化和非军事化,军民一体,联合作战,民众参与的程度比其他任何作战行动都大得多。

(10) 技术作用突出。技术是进出网络空间、实施心理进攻与防御的基本条件。只有拥有技术优势,才能控制网络,才能攫取信息优势;通过网络技术霸权,就能获取网络信息霸权。

#### 4. 网络空间心理战施加的影响和作用

网络空间心理战将对抗的战场进一步拓展到认知层,以信息对人的影响为武器,基于心理学原理和方法对敌方的认知、情感与意志施加影响,使敌方能够服从己方的意愿或者改变他们的行为。为了更有效地施加影响,网络空间心理战不但要利用多种形式的信息投送手段突破防御,将信息送到敌方群体,还需要结合心理学原理并采取多种心理战手段,才能达到预期的心理攻击效果。

控制思想是斗争胜利的最终目标,网络空间心理战是网络空间作战的高级形态,是未来作战的重要样式,是实施网络瘫痪战的重要手段,是削弱敌人整体作战效能的重要途径,

是影响敌人战争潜力发挥的重要因素。同时,网络空间心理战需要利用物理层和逻辑层的资源实现信号和信息传递,因此,其整体效能发挥离不开电子战、网络战,只有将多种作战样式有机结合才能完全掌握网络空间的控制权。

### 3.2.2 网络空间心理战对抗模型和武器体系

#### 1. 网络空间心理战对抗模型

网络空间心理战的武器是信息,其作用目标是敌方决策者、军队或民众,同时包括非参战国。从作战运用过程角度出发概括出的网络空间心理战对抗模型如图 3-1 所示。

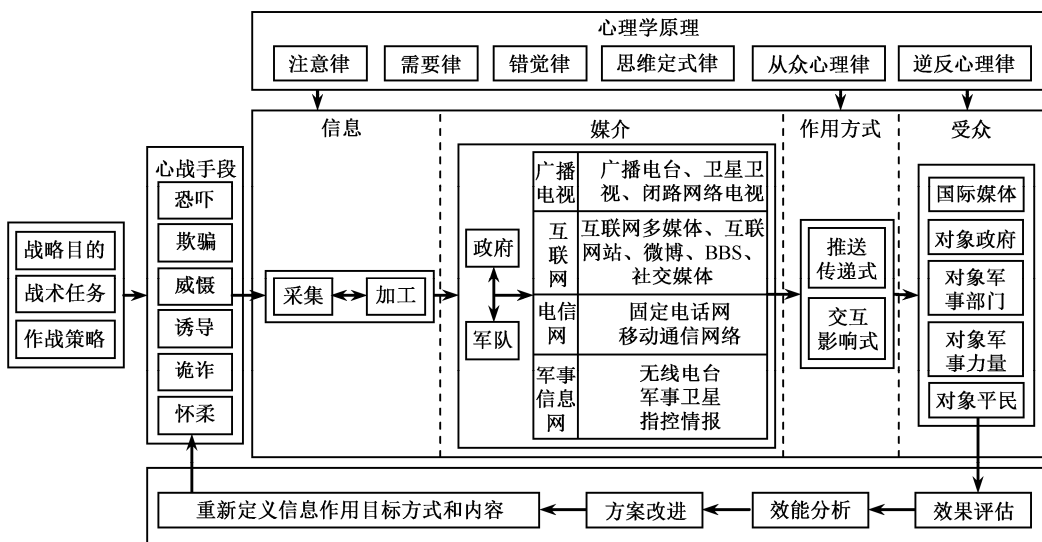


图 3-1 网络空间心理战对抗模型

进攻方要根据防守方的民族、文化地域特点,以及军事训练的薄弱环节等若干条件,结合战略要求进行战术安排,即将已经获得的相关信息进行有目的的加工处理。然后,结合实际网络空间环境条件对防守方目标进行区别化的心理打击,基本的信息传递媒介包括广播电视、互联网、电信网、军事信息网等,同时,也可能利用定向高功率微波、闾下刺激武器等毁伤型的网络空间心理战武器对防守方的认知功能实施打击。最后,需要根据实际产生的心理效果对作战方案进行效果评估,在效能分析阶段可以对不明确的心理影响因素进行测试性的局部战术动态评测,结合评测结果针对性调整心理攻击信息的逻辑内容、传输方式以及采取的手段等因素。实施网络空间心理战的过程中需要依照心理学原理设计,调整作战方案以提高对受众的影响效率。根据网络空间心理战信息传递和心理影响方式的差异,可将其网络空间心理战作用方式细分为两种。一种是推送传递式,依靠信息推送手段将准备好的各种形式的心理战信息送至受众,利用邮件、电话、视频等媒介的网络

空间心理战属于这一类型。这种作用方式受到媒介条件以及受众习惯等限制，进攻方难以迅速准确地获取受众反应，因此，对一次传递内容要求较高，作战效果不好把握，但受众数量多、范围大。另一种是交互影响式，依靠论坛、博客、微博等媒介的网络空间心理战属于这一类型。这种作用方式更注重与受众交互，进攻方通过回复、评论等能快速获取受众反应并据此进行战术技术调整，相对上一种作用方式，其反馈周期短、作战节奏快，而且由于是多次长期的影响，对一次传递内容的要求要低一些，最后的作战效果也比较容易把握，但受众数量较之推送传递式要少一些。

## 2. 网络空间心理战武器体系

结合网络空间心理战对抗模型和心理战特点，可以归纳出其武器体系。按照武器功能，网络空间心理战武器可分为指挥控制武器、主战武器和支撑保障武器等构成部分，如图 3-2 所示。另外，还可以按照武器形态分为固定、便携、车载、机载、舰载等，如图 3-3 所示。

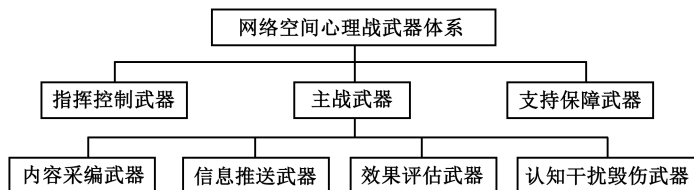


图 3-2 网络空间心理战按武器功能的武器体系

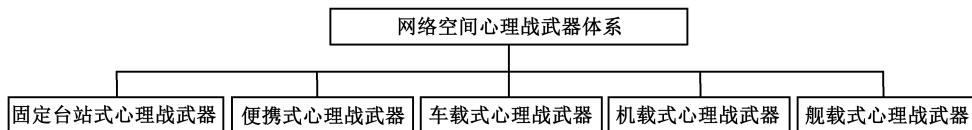


图 3-3 网络空间心理战按武器形态的武器体系

## 3. 网络空间心理战关键武器发展建议

现代信息战条件下，高度精确化、智能化、数字化和网络化的技术广泛运用，为心理战的信息收集、信息生成、信息处理、信息传输和信息显示提供了更先进、更快捷、更有效的物质技术手段，使网络空间心理战的渗透性、时效性、震撼性远远超过历史上任何一个时期，根据网络空间作战武器体系以及己方现状，目前应优先发展以下武器：

- (1) 互联网心理战武器。通过网络向互联网用户或用户群组推送图像、语音、文字、图片等多种形式的心理战信息，实现心理战作战目标。
- (2) 移动通信心理战武器。通过移动通信网络向手机终端推送心理战短信和彩信，进行心理战。
- (3) 网络空间心理战靶场武器。通过虚拟化、仿真和实装设备模拟或创建真实的网络空间心理战作战环境，支持网络空间心理战武器试验，支持网络空间心理战指战员实际作战技能和战略战术模拟训练及演习，支持网电空间心理战新技术试验。



### 3.2.3 网络空间心理战的主要手段

真正能够把物质空间与精神空间的对抗结合起来,还是现代的信息化战争。物质空间以其强大实力决定和影响着精神空间,精神空间又以其诱导劝服和分化瓦解等手段来放大物质空间搏杀的效果。精神空间中所使用的心理战手段,一方面是以信息媒体为基础的各种特定信息,主要包括各种思想、理论、观念、意见、要求、期望、劝告、口号和谣言等。另一方面是承载信息的媒介平台。在遂行心理战任务时,通过媒介平台可以将心理战信息转化为特殊形式的符号,并将这些符号承载的信息在终端向作战对象释放。常见的媒介主要有网络、电视、电话、广播、移动通信、卫星通信、数据通信、互联网、传单、报刊、音响等,随着科技的进步,媒介平台也在向智能、高速、一体方向发展。

心理战的实施必须依靠一定的手段。心理战手段的选择和运用,既要考虑心理战对象的特点,还要考虑信息媒介的因素。计算机网络以及网络空间的特点,对心理战手段的选择和运用都有直接的影响。在现代战争中,网络心理战一般采取以下手段进行。

#### 1. 进行网络心理宣传

在网络空间进行宣传具有众多的优越性,世界各国无不争先恐后地进入互联网抢占网络,争夺己方的宣传阵地。

##### 1) 组建心理战网站进行宣传

利用互联网组建专门网站进行宣传,是实施网络心理战的一个重要方式。互联网作为目前世界上最先进的宣传工具,具有信息传递实时精确、不受时间限制、阅读群体庞大等优点,成为网络心理战宣传的重要作战平台。但是,由于这种专门的心理战宣传网站带有明显的政治倾向性和官方性,易被对方识破,一定程度上影响宣传效果。

##### 2) 设置虚拟社区进行宣传

虚拟社区,是由互联网提供的一个供大家相互交流的场所,是对现实生活的支持和帮助。在网上,人们没有地域、年龄、国籍、地位等一切影响正常交流的障碍,人人完全平等,大家都可以自由地发表自己的言论,阐述自己的观点。它用各种各样的方法和设定,在非现实的空间中使人们的个性加以体现,使自己的理想得以实现。这样一种全新的虚拟社区性质决定了其拥有极高而且十分固定的访问量,这就为实施网络宣传心理战提供了极好的机会。

##### 3) 利用聊天室进行宣传

互联网聊天室人气旺,速度快,站点繁多,各种各样的聊天室令人目不暇接。为了吸引广大网络爱好者,不少聊天室,经常邀请著名的专家学者、政府官员、影视明星来当嘉宾,即所谓的“嘉宾聊天室”,让广大网民,围绕某一共同感兴趣的问题进行相互讨论,解答问题,倾听意见。种种聊天室的建立,为实施网络心理宣传提供了崭新、方便的空间。

可以设想,如果实施网络心理战宣传的组织或个人冒名顶替某位名人政要甚至国家元首与广大网民进行交流,并设法让网民相信,进而进行心理战宣传,那么其造成的影响将不可估量。

#### 4) 利用电子邮件进行宣传利用

利用电子邮件快捷、直观的特点,有针对性地对有关人员发送含有心理战信息的电子信件,从而影响其心理,这是网络心理战宣传的又一形式。在伊拉克战争中,美军利用其先进的设备和指挥控制系统,对伊拉克发起了以手机短信和电子邮件为主的网络攻势。从2003年1月6日起,美军就开始对伊拉克军队和地方官员发起电子邮件攻势,并向萨达姆亲信的移动电话发送短信。伊拉克很多军人、政府官员的手机上都接到了“我们知道你是谁,放下武器,别无出路”等信息。由于受强大心理宣传攻势的影响,有相当一部分伊拉克军人就偷越伊科边境向美军投降。

另外,还可以利用微信和QQ等进行心理战宣传。

## 2. 进行网络心理欺骗

进行网络心理欺骗是在计算机网络系统中所实施的信息欺骗。它通常包括三个方面的内容:对己方信息进行伪装;向敌方发送虚假信息;改变敌方信息流向,使敌方做出错误的判断和决策。在进行网络心理欺骗心理战中,网络宣传欺骗、“黑客”欺骗、病毒欺骗和电子邮件欺骗等都是常用的方式。

#### 1) 网络宣传欺骗

网络宣传欺骗就是通过网络有意识地散布大量虚假信息,以迷惑对手,混淆视听。由于利用网络进行宣传欺骗,所散布的信息能以图、文、声、像的多媒体形式出现,具有形象、生动、直观的特点,更具有迷惑性。从海湾战争、科索沃战争到伊拉克战争的一系列事实证明,网络宣传不仅能迷惑广大民众,有时候甚至可以改变历史,改变一个国家和地区的命运。

#### 2) “黑客”欺骗

利用“黑客”闯入对方计算机网络系统,输入虚假信息或篡改信息数据进行欺骗,是网络心理欺骗的重要形式。它通过网络某一节点,或以无线电通信方式把己方某些计算机与对方联网,或战前通过各种途径进入敌方指挥控制信息网络系统,把己方的虚拟信息,比如:虚假情报、假决心、假部署传输给敌方,迷惑敌人,诱敌判断失误;向敌方指挥官和士兵发布假命令,使敌听命于己,改变敌方指挥官的作战意图,使敌方军事陷入混乱。这种欺骗具有很大的迷惑性和破坏性。1995年美军组织了“联合勇士”演习,一名空军上尉军官就利用一根电话线和一个调制解调器,在众目睽睽之下入侵到大西洋舰队,成功地剥夺了指挥官的指挥权,向正在航行的舰队发号假指令,而那些接到指令的人却全然不知这个命令是假的。

### 3) 病毒欺骗

病毒欺骗是指设立逼真的“假网站”诱敌上钩,使其落入“病毒陷阱”,即以代理服务的方式,在网上建立一个与在线服务器内容相近且带毒的假目标,通过网上发布主页等途径,有意暴露进入端口,诱敌攻击,吸引和转移敌方攻击目标与方向,避免真实在线服务器遭受攻击。同时,组织力量对攻击之敌进行跟踪分析,了解掌握敌方攻击企图、实施攻击的手段和方法,研究制定有效的防护对策,以保护主要网站的安全运行。

### 4) 电子邮件欺骗

电子邮件欺骗的形式多种多样,常用的主要有两种:一种是在电子邮件中声明该邮件是来自系统管理员,要求用户修改口令,并威胁如果不服从则采取某种措施;另一种是电子邮件声称来自某一授权人,要求用户提供口令文件或其他敏感信息的拷贝。

## 3. 利用网络虚拟现实实施心理影响

随着网络技术的不断发展,利用网络虚拟现实技术制作“虚拟现实信息”,将成为网络心理战的利器。虚拟现实是计算机网络模拟的三维环境,是一种可以创建和体验虚拟世界的计算机网络系统。虚拟环境由计算机网络生成,它通过人的视觉、听觉、触觉等作用用于用户,使其产生身临其境的感觉的实景仿真。这种方法能使敌人在三维声、像环境中,看到酷似实物的立体图像,从而达到心理影响的效果。

利用虚拟现实技术,不仅可以创造“虚拟部队”“虚拟机群”“虚拟舰队”,而且还可以虚拟某国的部队在另一国的首都广场上进行阅兵的场景。甚至还可以虚拟某国的领导人发表不利于战争进行、影响士气的讲话,虚拟某国军队统帅宣布停战撤军的景象,还可以虚拟宗教全息圣像,动摇敌人的军心民心。美军已进行过这方面的试验。1993年2月,驻扎在索马里首都摩加迪沙以西15千米处,突然刮过一阵狂风,在沙土飞扬的昏暗空中,出现了一幅高达150~200米高的耶稣圣像,许多索马里信教军民纷纷跌倒在地进行祷告。事后证明,上述圣像正是虚拟现实图像,系美国协调机构驻索马里的心理战分队以试验为目的而施放的。1995年2月,美军为使海地临时军政当局交出政权,利用计算机虚拟技术,虚拟美军一架架战机进行空中编队后向海地猛扑过来,一艘艘战舰劈开海浪向海地包抄过来。当海地军政领导人从荧屏上看到这些景象后,顿时被这强大的军事威慑所慑服,立即表示同意交出政权。

### 3.2.4 网络空间心理战典型的几种武器

近些年来,西方国家耗巨资组建专业心理战部队,研发心理战武器器材,出现了一大批以信息为主导的新型心理战武器。这些武器通过光、声、电磁、气象和化学等手段,从心理上对敌方作战人员进行骚扰、恫吓、瓦解,使他们畏惧恐慌、精神崩溃、丧失斗

志。下面从电磁波武器、声波武器和光波武器三个方面来介绍网络空间心理战典型的几种武器。

## 1. 电磁波武器

电磁波辐射会对人体造成损伤，已被科学所证实。据中国电磁辐射测试中心经过的跟踪检测证实，超量的电磁辐射会造成人体神经衰弱、食欲下降、心悸胸闷、头昏目眩甚至脑部肿瘤等损伤。一些国家正利用这一原理，研制威力巨大的电磁武器，已经或比较常见的是利用无线电广播、电视进行心理宣传攻击和利用微波进行人脑控制等。

### 1) 无线电广播、电视进行心理宣传

早在二战时广播就被用作心理战武器，其成本低、覆盖广、受天气的影响小而且声音生动，可以平战结合，是战时可以“刺入敌人心灵的利剑”，也是和平时分化别国民心的“利刃”。它的不足在于模拟广播信号易被干扰，战时的无线电发射站易被攻击，而且受众还要有接收设备。在利用无线电广播进行心理宣传攻击方面，有很多成功的做法，其中比较著名的是美国之音。目前，几乎世界上所有有能力的国家都有对外的无线电广播，如 BBC、德意志电波、自由欧洲等。不仅如此，现在很多国家的心理战部队一般也都装备了可以随走随播的地面、空中移动广播设备。

电视不光可以被用来当作左右国内民意，调和国内矛盾的一种手段，而且它还可以进行进攻型的心理宣传。比如，1989 年东欧国家发生内乱时，西欧的电视机构就开始进行火上浇油的电视报道，扮演了非常不光彩的角色。

### 2) 微波武器

微波武器又被称为超高频武器，可以在人体的不同组织或器官中产生不同的效应。人体最易遭受电磁武器攻击的组织或器官是大脑、脖子、胸部和生殖腺。受到攻击时的症状是身心疲惫、记忆紊乱、皮肤生病、眼睛出血、白内障、角膜和视网膜损伤，甚至患癌症。

微波对人员的杀伤，其杀伤机理分为“非热效应”和“热效应”两类。非热效应是指当微波照射强度低时，使人的生理功能紊乱（如烦躁、头痛、记忆力减退、神经错乱以及心脏功能衰竭等），导致所操作或操纵的系统失灵。在 20 世纪 70 年代，美国就曾多次抗议苏联用微波照射美国驻莫斯科大使馆，使其工作人员的健康受到损害。热效应是指在高功率微波照射下，人的皮肤灼热，眼睛白内障，皮肤内部组织严重烧伤和致死等。苏联的研究人员曾把山羊当作“活靶”，进行强微波照射试验，结果 1 千米以外的山羊顷刻间“饮弹身亡”，2 千米以外的山羊顷刻丧失活动功能而瘫痪倒地。

微波心理战武器比较典型的是美国研制的首次正式承认的心理战武器“美杜莎”。其原理利用高频信号直接作用到人体大脑，使其产生莫名恐惧或出现幻听。由于此武器主要通过产生声波影响人体，声音出现在大脑内部，因此根本无法抵挡，对它束手无策。“美杜莎”是将声学 and 微波学连接到一起，主要影响人的心理，是非致命性的。但 3 毫米长波分子只要进入身体 0.3~0.4 毫米，皮下水和血分子瞬间就可以沸腾，这时人会感觉到尖利

疼痛,温度是 $45\sim 50^{\circ}\text{C}$ ,超过人体痛感极限,即使离开辐射区,痛感也不会消失。如果大脑经常受到这种声波影响,会产生中风现象,强大声波还会伴随大量热量,引起身体无法承受的痛感。

## 2. 声波武器

声波是机械纵波,它可以在固体、液体和气体中传播。人们日常可以听到的声音是 $20\sim 20\,000\text{kHz}$ 范围内的声波。目前,一些国家竞相开发研制声波武器。声波武器主要包括次声波武器、强声波武器、超声波武器、噪声波武器和声波定向武器等。

### 1) 次声波武器

频率低于 $20\text{Hz}$ 的就是次声波。次声波之所以会被用作军事武器,是因为次声波和人体器官固有频率相近,于是会产生共振,导致器官变形、移位甚至破裂,从而达到杀伤目的。次声波武器大体可分为两类:神经型次声波武器和器官型次声波武器。

神经型次声波武器的次声频率和人脑阿尔法节律( $8\sim 12\text{Hz}$ )很接近,次声波作用人体时便刺激人的大脑,引起共振,对人的心理和意识产生一定影响:轻者感觉不适,导致注意力下降、情绪不安、头昏、恶心;严重时使人神经错乱,癫狂不止,休克昏厥,丧失思维能力。

器官型次声波武器的次声频率和人体内脏器官的固有频率( $4\sim 18\text{Hz}$ )相近,会引起人的五脏六腑产生强烈共振。轻者肌肉痉挛,全身颤抖,呼吸困难;重者血管破裂,内脏损伤,甚至迅速死亡。

次声波武器的优点在于:

- (1) 突袭性强。次声波是常人听不到、看不见的,传播迅速,隐蔽性好。
- (2) 作用距离远。根据物理学原理,声波的频率越低,传播时介质对它的吸收就越小,波的传播距离也越远。
- (3) 穿透力强。传播介质对低频率的声波吸收较小,故次声波具有很强的穿透能力。实验表明,次声波能穿透几十米厚的钢筋混凝土。
- (4) 破坏性小。次声波在杀伤敌人的同时,不会造成环境污染,不破坏对方的武器,可作为战利品,取而用之。
- (5) 机动性较好。既可用于单兵作战,也可车载、机载。

法国科学家加夫雷奥认定,他发现了一种“全新的武器”,于是立即着手进行试验。他和同事们造了一个能发出次声波的“哨子”,并成功地将站在旁边的人全部“放倒”。当他和同事们将“哨子”的直径增至 $1.3$ 米时,所发出的次声波甚至撼动了整座大楼的围墙。他陆续研制出多种型号的声波武器,全部被列为法国军方的“最高机密”。加夫雷奥的实验室则被更名为“法国国防部次声波实验室”。

美国声波武器的研发和应用,堪称后来居上。在科索沃战争中,美军就曾使用次声波武器向敌方阵地发射次声波,使敌人在几秒钟内昏倒在地或呕吐不止,短时间内丧失了战斗力。

目前，次声波武器尚未真正在战场上使用，但确有一些国家在从事硬件器材、软件配置以及生物效应的试验。有的国家试验表明，10Hz、190 分贝的次声波，可使狗的呼吸发生困难甚至停止。次声波的强度越高，其杀伤力就越大。法国国防部次声波实验室已研究出三种形式的声波枪，即“哨子”“声学莱塞”和“风琴管声枪”，并称这三种武器可对工事、坦克甚至潜艇内的人员进行杀伤。

次声波武器虽是强大、厉害的武器，但却存在固有的缺陷。首先，次声波不易聚焦成束，且在空旷的环境中难以产生高强次声波；其次，次声波很长，因而定向困难；最后，它的聚焦尺寸太大，一般很难实现。更为致命的是“不分敌我”。

## 2) 强声波武器

强声波武器能发出足以威慑来犯者或使来犯者失去行动能力的强声波，而不会对人体造成长期的危害。它主要用于保护军事基地等重要设施。当有人靠近时，这种声学武器首先发出声音警告来人。如果来人继续靠近，声音就会变得令人胆战心惊。假如来人置之不理还继续逼近，这种声学武器就会使他们丧失行动能力。

## 3) 超声波武器

超声波武器能利用高能超声波发生器产生高频声波，造成强大的空气压力，使人产生视觉模糊、恶心等生理反应，从而使人员战斗力减弱或完全丧失作战能力。

2000 年，美国人伍迪·诺里斯发明了可以让攻击者“停下来”的非致命武器——“超声波子弹”。诺里斯解释说，超声波武器对大多数人来说，即便捂上耳朵，也会产生类似偏头痛的感觉，反应严重的人则会被击倒在地。

## 4) 噪声波武器

噪声波武器可以分为两种：一种是专门用来对准敌方指挥部的定向噪声波武器，它利用小型爆炸产生的噪声波来麻痹敌指挥人员的听觉和中枢神经，必要时可使人员在两分钟内昏迷。另一种是噪声波炸弹，它同样可以麻痹人的听觉和中枢神经，使人昏迷，主要用于对付劫机等恐怖分子。

## 5) 声波定向武器

声波定向技术的原理是利用特制的声波“聚焦”设备，将声音聚集为一束极为狭窄且几乎平行传输的声波后，“射向”选定的目标，向其传播特定信息。这种“定向”的声音，听起来就好像来自你的面前，而事实上它很可能是从几百米之外发出来的。利用这种技术在很远的距离对准某一个人说话，而周围的其他人根本听不到。

“声波定向”可以干扰敌人的判断力，让他们误以为有什么东西就在附近，而实际上听到的声音可能来自数百米之外的特制声波仪器。飞机的轰鸣声、隆隆的枪炮声、喧嚣的车辆声乃至嘈杂的人声都可以被“声波武器”射向敌军士兵或遍布战场各个角落。这样，

敌军士兵甚至敌军指挥部得到的是“大军压境”的信息，而实际上可能只是几台大功率的声波仪器在不断变换着战场声音的种类和强度。除此之外，微型“声波定向仪”发出的声音还可让分散行动的敌军士兵感到心惊胆战、精神错乱。这种对敌心理上的威慑效果可能是其他武器都难以达到的。

### 3. 光波武器

光波武器主要包括激光武器、幻觉炸弹等。

激光具有单色性，基谱线宽度很窄。普通光源中氩灯的谱线宽度为千分之五埃（1 埃= $10^{-10}$  米），氦氖激光器产生的激光谱线宽度只有千万分之一埃。就是说，激光的单色性比氩灯提高了几十万倍。激光能够向一个方向辐射，散开角度只有几分，甚至小到一秒。激光的高方向性使它在军事上很受重视。高度集束的激光，能量也非常集中。所以，激光作为武器，有很多独特的优点。首先，它可以用光速飞行，每秒 30 万千米。它一旦瞄准，几乎不要什么时间就立刻击中目标。另外，它可以在极小的面积上、在极短的时间里集中超过核武器 100 万倍的能量，还能很灵活地改变方向，没有任何放射性污染。

利用光波的有关特性，借助最新激光技术、全息技术，幻觉炸弹是能够使人产生幻觉形象的特种仪器，能影响人的神志、知觉，迫使人混淆现实与虚幻，并能借助特种设备发出指令。早在 20 世纪 90 年代中期，美国就成功进行了类似武器的非同寻常的试验，在虚拟战场上制造目标幻觉形象，包括飞机、坦克、舰艇、整支战斗部队等，也可制造各种有影响的人物形象。如海湾战争期间，美军利用激光心理战武器，向云端映射出伊斯兰殉教者的形象，并通过其向士兵喊话：“放下武器，回到真主那里去吧。”这种虚幻的“海市蜃楼”的心理战，无疑会对人的心理产生极大影响。

## 3.3 网络空间态势感知武器

网络空间态势感知武器主要实现网络感知、侦察和预警，及时搜集网络空间内的各种情报信息，并进行告警，具体包括：

- (1) 了解网络空间内友军、敌军及其他相关活动；
- (2) 评估友军网络作战能力；
- (3) 评估敌军网络作战能力和作战意图；
- (4) 评估友军和敌军的网络防御弱点；
- (5) 了解网络上的信息流，包括其目的和危险性；
- (6) 了解友军和敌军网络空间降级所带来的效果和任务影响；
- (7) 有效规划和执行网络对抗所需作战能力的可用性。

具体类型有网络扫描器、网络窃听器与工具、网络密码破译器、电磁侦测器和“爱因斯坦”计划等。下面分别加以介绍。

### 3.3.1 网络扫描器

#### 1. 工作原理

扫描器的工作原理就是模拟攻击者的手法主动地探测目标系统，发现和分析网络系统中可能存在的各种安全隐患，将扫描结果报告给用户，并向用户提供该漏洞的相应解决方法，从而提高网络和系统的安全，保证网络免遭恶意用户再次利用该漏洞实施攻击。扫描器工作原理如图 3-4 所示。

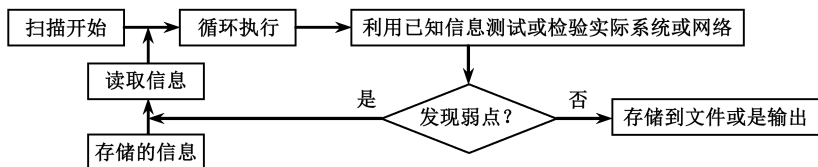


图 3-4 扫描器工作原理

#### 2. 侦察扫描

侦察扫描是利用各种网络协议产生的数据包以及网络协议本身固有的性质进行扫描。目的是确认目标系统是否处于激活状态，获取目标系统信息。常用的扫描方法有 Ping Sweeps、UDP Sweeps、操作系统确认扫描等。

##### 1) Ping Sweeps (Ping 扫描方式)

Ping Sweeps 是简单发现一个 IP 范围内的主机是否处于激活状态的扫描方法，有三种 Ping 扫描方式。

第一种是简单发送因特网控制报文协议 (ICMP, Internet Control Messages Protocol) ECHO 请求，然后等待 ICMP ECHO 应答。如果收到了应答，就认为目标是激活状态。其实就是使用常规的 Ping 命令。如果想阻止对这样的 ICMP ECHO 应答，只需要禁止 ICMP ECHO 即可。

第二种是广播 ICMP。向整个局域网发送 ICMP ECHO 请求。这样的请求会被广播到整个局域网，网中激活的主机会回送 ICMP ECHO 应答。UNIX 系统对于请求常常回送网络地址，而 Windows 系统常常是忽略。

第三种是 Non-ECHO ICMP。阻止前来的 ICMP ECHO 是不够的，可以使用 Non-ECHO ICMP 协议收集一个系统的信息。例如，使用 ICMP type13 消息 (时间戳) 以及 ICMP type17



消息（地址掩码请求）。用 ICMP 时间戳请求和应答你可以得到目标的时间；ICMP 地址掩码请求，可以在无盘系统启动引导程序时，得到它的网络掩码。可以用 `icmpush & icmpquery` 工具来实现这样的扫描。许多防火墙通过配置只是阻止 ICMP ECHO 扫描，而没有阻止 `icmpush & icmpquery` 工具的扫描。

## 2) UDP Sweeps (UDP 扫描方式)

用户数据报协议（UDP，User Datagram Protocol）扫描与 TCP 扫描相比不是很容易实现的，因为它是无连接协议，又可能被路由器丢弃。如果一个 UDP Sweeps 的端口不是处于激活状态，目标会发回一个 ICMP Port Unreachable 应答消息。但是，许多的 UDP 服务并不对 UDP Sweeps 应答，送回来的也许是 UDP Port Unreachable，这就说那个 UDP 端口没有开放。而且对于防火墙来说，UDP 数据包也可能被故意丢弃的，所以使用 UDP 扫描是非常不可靠的。但是，UDP 扫描有一个好处就是能够使用。

IP 广播地址，一个允许 UDP 数据包的网络，可以通过送一个 UDP 数据包到一个广播地址的高端端口。如果那个端口没有过滤掉这个 UDP 数据包，那么扫描者就可以得到许多从目标网络得到的 ICMP Port Unreachable 消息。

## 3. 端口扫描

端口扫描向目标主机的 TCP/IP 服务端口发送探测数据包，并记录目标主机的响应。通过分析响应来判断服务端口是打开还是关闭，就可以得知端口提供的服务或信息。一个端口就是一个潜在的通信通道，通过端口扫描，可以得到许多有用的信息，从而发现系统的安全漏洞。端口扫描也可以通过捕获本地主机或服务器的流入流出 IP 数据包来监视本地主机的运行情况。通常分为 TCP 扫描、文件传送协议（FTP，File Transfer Protocol）反弹扫描、源端口扫描。

### 1) TCP 扫描

TCP 扫描一般都是根据 TCP 数据的设置、三次握手中的交互出现的问题来扫描的。TCP 端口扫描方式有以下几种：

（1）TCP Connect 扫描。这是最简单的扫描方式，利用 TCP 协议的三次握手。扫描者发送一个 SYN 数据包，等待目标机反应。如果目标机返回的是 SYN/ACK 数据包，证明目标端口处于监听状态；如果返回的是 RST/ACK 数据包，证明目标端口不处于监听状态，而且连接将被置为 RESET；即该端口不开放。当收到 SYN/ACK 时扫描者再发送 ACK 数据包，就完成一次完全连接。

（2）TCP SYN 扫描。这种技术通常认为是“半开放”扫描，这是因为扫描程序不必打开一个完全的 TCP 连接。扫描程序作为客户端，不发送最后一个 ACK 包，这样服务器端认为没有建立一次 TCP 连接，因此不会在系统的审计记录中留下痕迹。

（3）TCP FIN 扫描。FIN 扫描使用 FIN 数据包。扫描者使用 FIN 数据包等待目标应答。如果该端口是开放的，则这个 FIN 包被忽略。如果该端口是关闭的，则返回一个 RST 包。

通过识别这种差别，扫描程序就可以判断出端口的开放情况。

(4) TCP Fragmentation 扫描。前几种扫描方式都不能通过防火墙，因为防火墙通常只允许以少数几个端口为目的端口的 TCP 报文通过，这样无法达到大面积的扫描目的。但通过把一个 TCP 报文分割到多个 IP 包中，可使防火墙无法从一个 IP 包中找到完整的 TCP 报头，从而无法进行过滤。

上述几种扫描方式中，方法(1)不需要特殊权限；方法(2)、(3)和(4)都需要程序打开 Raw socket，自己拼装 TCP/IP 包，这是需要超级用户权限的。

## 2) FTP 反弹扫描

FTP 反弹扫描主要利用 FTP 协议中对代理 FTP 这一特性，对 FTP 服务器进行欺骗扫描。FTP 服务器作为反弹代理，黑客能够进行掩饰源扫描地址的端口扫描。即让 FTP 服务器做“代理”，将一组字符发到特定服务器的 IP 地址和端口。如果要执行 FTP 反弹扫描，中间 FTP 服务器必须提供一个可读写的目录。

## 3) 源端口扫描

源端口扫描主要通过扫描 DNS、SMTP、HTTP 这些默认端口，来判断其打开情况。可使用的工具有 SuperScan，并且集成了 whois 查询等实用功能。Windows 平台下的有 Nmap 和 X-Scan。黑客种植木马前会进行此类扫描。

# 4. 漏洞扫描

通过漏洞扫描在获得目标主机 TCP/IP 端口和其对应的网络访问服务的相关信息后，将这些信息与网络漏洞扫描系统提供的漏洞库进行匹配，如果满足匹配条件，则说明漏洞存在。或者通过模拟黑客的攻击手法，对目标主机系统进行攻击性的安全漏洞扫描，如测试弱口令等。若模拟攻击成功，则表明目标主机系统存在安全漏洞。漏洞扫描可分为系统漏洞扫描和 Web 漏洞扫描。前者主要针对网络操作系统，而后者主要针对网络应用程序。从实现技术上分为基于网络系统漏洞库规则的匹配技术和基于插件程序结构的外部测试脚本技术。

## 1) 基于网络系统漏洞库规则的匹配技术

基于网络系统漏洞库的漏洞扫描主要依赖于所使用的漏洞库。通过采用基于规则的匹配技术，即根据安全专家对网络系统安全漏洞、黑客攻击案例的分析和系统管理员对网络安全配置的实际经验，可以形成一套标准的网络系统漏洞库，然后在此基础上构成相应的匹配规则，由扫描程序自动地进行漏洞扫描的工作。这种漏洞扫描器是基于浏览器/服务器结构。它的工作原理是：当用户通过控制平台发出了扫描命令之后，控制平台即向扫描模块发出相应的扫描请求，扫描模块在接到请求之后立即启动相应的子功能模块，对被扫描主机进行扫描。通过分析被扫描主机返回的信息进行判断，扫描模块将扫描结果返回给控制平台，再由控制平台最终呈现给用户。

这种技术的有效性主要取决于漏洞库的完整性。对于黑客所探知的未知漏洞，由于没有包含在漏洞库中，其防御性则大幅度降低。另外，漏洞库的修订和更新的性能也会影响漏洞扫描系统运行的时间。因此，漏洞库的编制不仅要每个存在安全隐患的网络服务建立对应的漏洞库文件，而且应当满足前面所提出的性能要求。

## 2) 基于插件程序结构的外部测试脚本技术

插件技术针对某一具体漏洞，编写对应的外部测试脚本。通过调用服务检测插件，检测目标主机 TCP/IP 不同端口的服务，并将结果保存在信息库中，然后调用相应的插件程序，向远程主机发送构造好的数据，检测结果同样保存于信息库，以给其他的脚本运行提供所需的信息。如果插件编写规范，用户自己可以用 Perl、C 或自行设计的脚本语言编写的插件来扩充漏洞扫描软件的功能，使漏洞扫描软件具有可扩展性。

插件是由脚本语言编写的子程序，扫描程序可以通过调用它来执行漏洞扫描，检测出系统中存在的一个或多个漏洞。添加新的插件就可以使漏洞扫描软件增加新的功能，扫描出更多的漏洞。这种技术使漏洞扫描软件的升级维护变得相对简单，而专用脚本语言的使用也简化了编写新插件的编程工作。

## 3.3.2 网络监听器与工具

### 1. 网络监听工具的概念

网络监听工具是网络管理员常用的一类管理工具。使用这种工具，网络管理员可以监视网络的状态、数据流动情况以及网络上传输的信息。但是网络监听工具也是黑客的常用工具。当信息以明文的形式在网络上传输时，便可以使用网络监听的方式来进行攻击。将网络接口设置为监听模式，便可以源源不断地将网上传输的信息截获。

网络监听可以在网上的任何一个位置实施，如局域网中的一台主机、网关或远程网的调制解调器之间等。黑客用得最多的是截获用户的口令。

当黑客成功登录一台网络上的主机，并取得了该主机的超级用户权限后，往往要扩大战果，尝试登录或夺取网络中其他主机的控制权。而网络监听则是一种最简单且最有效的方法，能轻易地获得用其他方法很难获得的信息。

在网络上，监听效果最好的地方是在网关、路由器、防火墙一类的设备处，通常由网络管理员来操作。使用最便捷的地点是在一个以太网中的任何一台上网的主机上，这是大多数黑客的做法。

### 2. 网络监听的基本原理

以太网是目前应用最广泛的局域网拓扑，以太网协议的工作方式是将要发送的数据包发往连接在一起的所有主机，在包中包含着应该接收数据包的主机的正确地址。所以，只

有与数据包中目标地址一致的那台主机才能接收该数据包。但是当主机工作在监听模式下，不管数据包中的目标物理地址是什么，主机都将接收。

在互联网上有很多使用以太网协议的局域网，多台主机通过通信线路、集线器连接在一起。当同一网络中的两台主机通信的时候，源主机将写有目标地址的数据包直接发往目的主机。但这种数据包不能在 IP 层直接发送，必须从 TCP/IP 协议的 IP 层交给网络接口，即数据链路层，而网络接口是不会识别 IP 地址的，因此在网络接口数据包增加了一部分以太帧头的信息。在帧头中有两个域，分别是只有网络接口才能识别的源主机和目标主机的物理地址，这是一个与 IP 地址对应的 48 位的地址。在传输数据时，包含物理地址的帧从网络接口发送到物理连线上，如果局域网是由一条电缆连接而成，则信号在电缆上传输，能够到达线路上的每一台主机。如果使用集线器，由集线器再发向连接在集线器上的每一条线路，信号也能到达连接在集线器上的每一台主机。当信号到达某一台主机的网络接口时，正常情况下，网络接口读入数据帧并进行检查，如果数据帧中携带的物理地址是自己的或者广播地址，则将数据帧交给上层协议软件进行处理，否则丢弃该数据帧。

然而，当主机工作在监听模式下，所有的数据帧都将被交给上层协议软件处理。而且，当连接在同一条电缆或集线器上的主机被划分为几个子网的时候，如果一台主机处于监听模式下，它还将接收到发往与自己不在同一个子网的主机的数据包。也就是说，在同一条物理信道上传输的所有信息都可以被接收。

### 3. 网络监听工具

网络监听技术发展到现在，产生了一些可工作在各种平台上的相关软硬件工具，其中有商用的，也有免费的。Windows 平台下有 WinDump 和 Iris Eeye 等，UNIX 平台下有 Snoop、Tcpdump、Ngrep、Dsniff、Ettercap 和 Sniffit 等。其中，WinDump 是 Tcpdump 的 Windows 移植版，采用命令行方式运行。Iris Eeye 是一款付费软件，完全图形化界面，可以很方便地定制各种截获控制语句，对截获数据包进行分析、还原等。

### 4. 监听器

#### 1) 分类

监听器分为手机监听器、电话监听器、无线监听器、车用数码监听器、密码监听器等，在生活中大多数人使用的是手机，因此手机监听器被视为一块大肥肉，很多人为了利益而积极研制开发更加简单安全的民用手机监听器。

#### 2) 手机监听器

(1) 软件型骇客手机。它属于一种手机窃听器，通过监听软件来实施，此方法只可以监听被监听人的一部手机。此软件可以在网上免费下载，它只是一款用于侦测手机噪声的应用软件而已。

(2) 芯片型骇客手机。通过加装芯片实现监听，它同样只可以监听一部手机。

(3) 专业手机监听器。以色列生产的专业手机监听器，拦截距离可达上万千米，但是

它已经不是在手机与基站间进行拦截了，它的有效监听距离，与地球同步通信卫星信号覆盖范围几乎相同，但只可监听全球移动通信系统（GSM，Global System for Mobile communication）制式手机。

### 3) 专用监听器材

这类器材是军用及间谍使用器材，对通信信号的拦截时间只需要几十纳秒，价格比较贵。

（1）主动式监听器。它可截获被监听手机的一切资料，并且可以盗用被监听号码作为主叫或被叫，总之，可以行使被监听手机的一切功能。

（2）被动式监听器。所谓的“监听王”就属于这种被动式监听器，由于受监听距离的限制，实际没有多大用处，所以即使公安机关也不采用这种设备，他们需要监听时都是在检察院授权之后，委托电信部门去进行，当然这也是法律规定的。

主动式监听器和被动式监听器有一共性，就是在启动监听设备后，必须与被监听手机同处在同一个基站内，这也就是说，它们都是受距离限制的，并非像某些人夸张的那样，可以无距离限制地进行电话监听，而且码分多址（CDMA，Code Division Multiple Access）在监听开始时有几秒钟时间的监听滞后。

网络监听是一把双刃剑，总是扮演着正反两方面的角色。对于网络管理员来说，网络监听技术可以用来分析网络性能，对检查网络是否被入侵发挥着重要的作用；对于入侵者来说，网络监听技术可以很容易地获得明文传输的密码和各种机密数据。为了保护网络信息的安全，必须采用网络监听技术进行反跟踪，时刻探明现有网络的安全现状，掌握先机，才能保证网络的信息安全。

## 3.3.3 网络密码破译器

网络密码破译器是能从敌对网络所截获的密文中推断出原来的明文的软件或工具，功能强大的网络密码破译器还能采用删除、更改、增添、重放、伪造等方法向密文中加入假消息。理论上讲，任何密码都是可以破译的。在实际环境中是否需要设法去破译，主要取决于：破译的代价是否大于可能获得的结果；破译的时间是否大于结果的有效期；是否能产生足够多的数据供破译使用。

### 1. 密码破译技术概念

密码破译技术是指实施密码破译过程中常用的各种技术、手段、措施、方法和工具。

在计算机网络传输过程中，除了合法的接收者，还有非授权者，非授权者通过各种办法在信息传输过程中截取信息（如搭线窃听、电磁窃听、声音窃听等来截取机密信息），因此机密信息在网络中传输通常要进行加密，但有时还是能够被非授权用户截获，通过密

码破译获得明文甚至是密钥，使机密泄露。

## 2. 密码破译的主要因素

密码破译的主要因素为：

第一个因素是算法的强度。例如，除了尝试所有可能的密钥组合之外的任何方法都不能使信息被解密。

第二个因素是密钥的保密性。数据的保密程度直接与密钥的保密程度相关，注意区分密钥和算法，算法不需要保密，被加密的数据是先与密钥共同使用，然后再通过加密算法。

第三个因素是密钥长度。密钥的长度以“位”为单位，根据加密和解密的应用程序，在密钥的长度上加上一位则相当于把原来可能的密钥的总数乘以 2。简单地说，构成一个任意给定长度的密钥的位的可能组合的个数可以被表示为 2 的  $n$  次方，这里的  $n$  是一个密钥长度，因此，一个 40 位密钥长度的配方将是 2 的 40 次方或万亿种可能的不同的密钥，与之形成鲜明对比的是现代计算机的速度。

## 3. 密码破译方法

通常，密码破译有下列方法。

### 1) 密钥的穷尽搜索

破译密文最简单的方法，就是尝试所有可能的钥匙组合。假设破译者有识别正确解密结果的能力，经过多次密钥尝试，最终会有一个钥匙让破译者得到原文，这个过程就称为密钥的穷尽搜索。

### 2) 密码分析

在不知其钥匙的情况下，利用数学方法破译密文或找到钥匙的方法，称为密码分析。密码分析有两个基本的目标：利用密文发现明文；利用密文发现钥匙。根据密码分析者破译（或攻击）时已具备的前提条件，通常将密码分析攻击法分为 4 种类型。

（1）唯密文破解。在这种方法中，密码分析员已知加密算法，掌握了一段或几段要解密的密文，通过对这些截获的密文进行分析得出明文或密钥。唯密文破解是最容易防范的，因为攻击者拥有的信息量少。但是在很多情况下，分析者可以得到更多的信息。如捕获到一段或更多的明文信息及相应的密文，也是可能知道某段明文信息的格式的。

（2）已知明文的破译。在此方法中，密码分析员已知加密算法，掌握了一段明文和对应的密文。目的是发现加密的钥匙。在实际使用中，获得与某些密文所对应的明文是可能的。

（3）选定明文的破译。在这种方法中，密码分析员已知加密算法，设法让对手加密一段分析员选定的明文，并获得加密后的密文。目的是确定加密的钥匙。差别比较分析法也是选定明文破译法的一种，密码分析员设法让对手加密一组相似却差别细微的明文，然后比较他们加密后的结果，从而获得加密的钥匙。

(4) 选择密文攻击。密码分析者可得到所需要的任何密文所对应的明文(这些明文可能是不明了的),解密这些密文所使用的密钥与解密待解的密文的密钥是一样的。它在密码分析技术中很少用到。

上述4种攻击类型的强度按序递增,如果一个密码系统能抵抗选择明文攻击,那么它当然能够抵抗唯密文破解和已知明文破解。

#### 4. 其他密码破译方法

除密钥的穷尽搜索和密码分析外,实际生活中,破密者还可能针对人机系统的弱点进行攻击,而不是攻击加密算法本身。

利用加密系统实现中的缺陷或漏洞等都是破译密码的方法,虽然这些方法不是密码学所研究的内容,但对于每一个使用加密技术的用户来说是不可忽视的问题,甚至比加密算法本身更为重要。常见的方法有:

- (1) 欺骗用户口令密码。
- (2) 在用户输入口令时,应用各种技术手段,“窥视”或“偷窃”密钥内容。
- (3) 利用加密系统实现中的缺陷。
- (4) 对用户使用的密码系统偷梁换柱。
- (5) 从用户工作生活环境获得未加密的保密信息,如进行“垃圾分析”。
- (6) 让口令的另一方透露密钥或相关信息。
- (7) 威胁用户交出密码。

#### 5. 防止密码破译的措施

防止密码破译,除我们要从思想上加以重视外,采取的具体措施如下:

(1) 强壮加密算法。通过增加加密算法的破译复杂程度和破译的时间,进行密码保护。如加长加密系统的密钥长度,一般在其他条件相同的情况下,密钥越长破译越困难,而且加密系统也就越可靠。

(2) 动态会话密钥。每次会话所使用的密钥不相同。

(3) 定期更换加密会话的密钥。

### 3.3.4 电磁侦测器

电磁侦测器能对敌方计算机网络系统内各种电子设备所发射或辐射的电磁信号进行搜索、定位、检测、识别、记录和分析,获取对方计算机信息系统内的有关信息和情报。

任何一台电子设备工作时都会产生电磁辐射,计算机及其网络设备也不例外。计算机设备包括主机显示器、磁盘机、磁带机、终端机、打印机等所有设备所传递的数字脉冲信号都含有丰富的谐波,频谱可伸展到甚高频(VHF, Very High Frequency)和超高频(UHF,

Ultra High Frequency) 范围, 不论辐射能力强弱, 都会不同程度地产生电磁辐射, 泄露信息。计算机信息泄露, 主要有两种途径: 一是被处理的信息会通过计算机内部产生的电磁波向空中发射, 称为辐射发射; 二是这种含有信息的电磁波也可以经电源线、信号线、地线等导体传送和辐射出去, 称为传导发射。计算机电磁辐射尤其以带阴极射线管的视频显示器最为严重, 屏幕上显示的信息, 在很远的地方用高灵敏度电磁侦听器, 不需要用复杂的分析技术就可以直接接收下来。据了解, 国外已能做到在 1 千米外同时侦听 20 台正在工作的计算机的辐射信息。这种侦察就已经不限于为网络攻击做准备, 而是可以直接从敌计算机网络截获有关情报信息。

### 3.3.5 “爱因斯坦”计划

#### 1. 简介

“爱因斯坦”计划, 即国家网络安全保护系统 (NCPS, National Cybersecurity Protection System), 起源于美国国土安全法和联邦信息安全管理法案, 由美国联邦政府主导的一个网络安全自动监测项目, 用于监测政府网络入侵行为, 保护政府网络系统安全。一旦遭受网络攻击, 监测系统将自动向国土安全部下属的美国计算机应急响应小组 (CERT, Computer Emergency Response Team) 报警。简而言之, 它是一个政府主导, 各商业机构参与的国家级大项目, 并在法律上由美国政府签署该投资, 美国国家安全局全面执行的跨度大、项目众多的国家计划。

目的是把美国联邦机构各自的互联网出口数据汇集并分析、感知, 获取整个联邦政府的安全态势, 提高相互之间的信息共享、信息安全的协同。美国国土安全部通过“爱因斯坦”计划自动高效地去收集、关联、分析和共享通信数据, 感知网络中的各种威胁行为, 从而采取对策。安全专家可以通过“爱因斯坦”计划实时纵览跨机构的安全事件, 采取应急处置措施。各成员组织也可以访问安全网站查看相关网络数据。

“爱因斯坦”计划包括 1、2、3 个计划。在 2010 年的 RSA 大会 (全球信息安全大会) 上, 前美国总统奥巴马的网络安全协调官霍华德·施密特宣布针对美国《国家网络安全综合计划》(CNCI) 秘密文件公布一份 5 页的摘要解密文件。这个文件介绍了 CNCI 的 12 项计划, 其中, 两项计划是升级和翻新政府的网络监控系统, 一项是计划 2: 部署基于入侵检测系统 (IDS, Intrusion Detection System) 的“爱因斯坦”-2 系统; 另一项是计划 3: 部署基于入侵防御系统 (IPS, Intrusion Prevention System) 的“爱因斯坦”-3 系统。美国政府期望通过“爱因斯坦”计划的实施, 具备更快速地应对网络威胁进行检测和响应的能力。

“爱因斯坦”计划的实施引起了国际社会的广泛关注, 特别是“爱因斯坦”-3 不仅部署在联邦政府网络, 还部署到了公共互联网络上, 并且强调网络态势感知和实时处置能力。它采用何种技术, 获取哪些信息, 有何处理能力以及准备如何使用, 都成为大家关心的问题。



## 2. 负责机构

“爱因斯坦”计划是由美国国土安全部负责，美国国防部和国家安全局参与的网络安全示范和推广工程。

国土安全部下属 26 个部门中的 2 个部门在网络安全策略和计划执行中起着举足轻重的作用：科学与技术局和国家保卫与计划执行局。科学与技术局偏重于中长期的研究，国家保卫与计划执行局则注重目前和短期计划执行。科学与技术局归纳和定义主要的安全问题，国家保卫与计划执行局以解决这些问题为任务目标。尽管有明确分工，但是“网络感知”却是这两个部门的共同工作重点。

国家保卫与计划执行局下属的 US-CERT 由 4 个部门和一个中心组成，其中的“态势感知部”具体负责“爱因斯坦”计划的实施。

## 3. 系统能力及特点

该系统可以对网络数据包进行实时、深度检查，能检测包括电子邮件附件在内的任何网络数据流内容，实现在网络空间威胁造成实际危害之前，自动完成检测，对恶意网络流量进行特征提取和识别，并相应做出合适的处置。主要有以下三个特点：第一，可以基于已知威胁的相应处理模式，通过预先确定的入侵威胁行为特征来触发报警，并进行数据捕获分析。第二，可以通过基于对网络数据特征、行为、协议或流量信息实时监测，实现对网络系统中异常行为的报警。第三，能够支持动态防御，强化与执法部门和情报机构在情报搜集、技术分析、计算机犯罪取证的协作，吸收政府信息资产的相关私营企业和组织共同参与，有效确保网络空间威胁预警信息分发和协调网络安全事件应急处置。

## 4. 系统工作步骤

该系统的工作步骤是：收集网络异常行为数据；对数据进行分析，获取异常行为信息；通过国家网络安全和通信集成中心与政府机构合作，进一步确定异常活动直接相关的网络运行情况；向相关机构提出配置管理和应急处理措施建议。

例如，如果美国某政府部门有几台计算机感染了计算机蠕虫病毒，恶意代码随即开始自动扫描网络连接，力图感染其他计算机，以构建一个僵尸网络。当病毒扫描到其他政府部门的网关时，装载的“爱因斯坦”计划流量监测系统一旦探测到异常流量，立即触发“爱因斯坦”计划的警报系统。当计算机应急响应小组确定了受感染的计算机 IP 地址后，就会马上切断网络连接并运行杀毒程序予以查杀。

## 5. “爱因斯坦”计划的工作思路

国家统筹规划、统一部署，对政府部门互联网出入口进行统一归并。互联网出入口与城堡的城门类似，城门越多，需要防御的点就越多，潜在的漏洞与风险就越大。美国政府对政府部门的互联网接入口进行缩减，实施集中监控，既便于统一管理，又可以有效降低遭受网络攻击的风险，提升安全防御能力。但美国政府推动该计划也不是一蹴而就的，而是根据实际情况，逐步推进“缩口子”，既确保计划顺利实施，又保证联邦政府工作平稳运行。

统一建设信息安全基础设施，依照职能分工实现部门联动和资源共享。“爱因斯坦”计划部署实施之前，美国各部门在安全保密领域各自为政，防范网络攻击的能力和水平参差不齐，一旦遇到大规模攻击窃密，就会显得力不从心。通过建立统一的网络监测和安全预警基础设施，采用标准统一的工具进行配置和监控，确保了网络环境安全的一致性，既可以及时发现网络攻击、窃密与泄密事件，也可依靠专业队伍及时有效应对，大幅提升了政府互联网整体安全态势感知和入侵防御能力，相当于在网络世界中建立了一套“爱国者导弹防御系统”。

## 6. 部署进程

“爱因斯坦”计划目前由 3 个实施阶段组成：

### 1) “爱因斯坦”-1

“爱因斯坦”-1 系统于 2003 年开发，部署时间截止到 2008 年年底，由马里兰州的开源安全公司采用商业技术开发。

“爱因斯坦”-1 是一个被动型的数据流跟踪监视系统，记录连接到美国联邦政府网络计算机的 IP 地址、通信端口、通信时间，以及联邦网络目标计算机的互联网协议地址、通信协议、通信端口等信息，并对这些信息进行收集、管理、分析和共享。通过该计划，能够建立和增强对美国网络空间态势感知的能力；能够从更多的方面帮助联邦政府进行蠕虫检测，尤其可以形成一幅跨政府部门的蠕虫攻击图；通过跨政府部门的带内和带外的异常行为分析，能够更加全面地分析异常行为，并对其他部门提供预警信息和攻击线索；能够为联邦政府机构提供更有价值的配置管理建议；能够从整体上了解政府网络的健康度。

### 2) “爱因斯坦”-2

“爱因斯坦”-2 通过分布式的入侵检测系统建立一套安全监测系统，形成美国政府网络空间安全的早期预警体系。当网络流信息进入或离开政府网络时，数据流的备份就会被传送到“爱因斯坦”-2 系统。如果“爱因斯坦”-2 发现数据流包含恶意代码，即发出告警。然后，US-CERT 对可疑数据进行分析处理，同时将受到攻击或感染病毒的目标计算机脱线，清除恶意代码后再重新上线。

“爱因斯坦”-2 计划是 1 号计划的增强，部署时间为 2008 年到 2010 年。该计划系统具有启发性，有助于分析人员识别攻击手段和特定攻击目标，对网络威胁的响应速度明显提高。“爱因斯坦”-2 还可以提供源数据的相关性和可辨性，这将极大地提高 US-CERT 的分析师对网络环境的认知能力，有利于掌握联邦政府网络的总体安全态势，增强其处置网络安全的弱点和漏洞的能力，并使 US-CERT 能够更加有效地为美国各级政府的网络安全防御部门、私营部门的安全专家以及美国公众分享相关的安全信息。

### 3) “爱因斯坦”-3

“爱因斯坦”-3 是入侵防范系统，旨在保护美国民用部门和联邦行政机构的网络安全。

它使用基于威胁的签名技术，对进出联邦行政机构网络的所有数据包进行实时监测，并判断其是否具有威胁性。

“爱因斯坦”-3 的目标是确认恶意网络流量并鉴别其特性，以增强网络安全分析能力、安全态势感知及安全响应能力。“爱因斯坦”-3 主要解决的问题是网络空间威胁，包括钓鱼、IP 欺骗、僵尸网络、DoS、DDoS、中间人攻击，以及其他恶意代码插入等。国家安全局为“爱因斯坦”-3 提供关键技术支持，从截获的各种网络威胁当中判定和提取特征，并加入“爱因斯坦”-3 特征库。“爱因斯坦”-3 还可以在危害发生前，自动检测并正确响应网络威胁，最终形成一个支持动态保护的入侵防护系统，它还支持加强国土安全部与联邦行政部门和机构之间的信息共享，赋予国土安全部在检测到网络入侵时自动警告的能力。

在每个政府部门网络的出口部署入侵防御系统，形成各自的个体保护。其主要“创新”在于强调面向网络的实时态势分析、威胁感知、主动防御、部署方式和运作流程。“爱因斯坦”-3 具有实时深度检测并进行威胁处置的能力，系统发现可疑活动，立刻与后端的智能系统联动分析，并根据反馈实施管控。

从 2009 年开始，“爱因斯坦”计划并入 CNCI；2010 年，US-CERT 公布“爱因斯坦”-3 演习程序，分成 4 个连续阶段，时长 18 个月；2011 年“爱因斯坦”-3 进入实用阶段并全面部署。2012 年，国土安全部提出的该计划预算为 3 亿美元，用于安全风险评估、改进、队伍建设培训、合作协调等。2016 年国土安全部（DHS）提交了一份总额达 650 亿美元的 2016 财年预算申请，并重点支持 NCPS 及持续诊断和缓解项目（CDM），以加强网络空间的态势感知和信息分享能力。

## 7. “爱因斯坦”-3 的演习

“爱因斯坦”-3 部署期间，美国国土安全部安排了一些演习以验证可能使用的技术。演习中测试了现有系统之间的改进互补，包括“爱因斯坦”-1 和“爱因斯坦”-2 以及由国家安全局所研发技术的部署。该演习的目的是检验“演习技术”的能力：在某政府部门和指定的互联网连接访问运营商之间传输的互联网流量经过选择和重定向；由 US-CERT 运用入侵检测和防御技术进行监测，对预设的网络威胁产生自动报警。

“爱因斯坦”-3 演习分为四个连续的阶段，见表 3-1。

表 3-1 “爱因斯坦”-3 演习安排

阶段	检验目标	测试目的	持续时间
1	网络运营商	在网络中识别特定的数据流并重定向到指定的节点，再传入网络后重复识别和重定向	
2	AT&T 公司	部署安装在网络运营商的网络节点	30 天
3	“演习技术”	对特定的数据流检测，反制已知或疑似的网络威胁	60 天
4	“评估结果”	评估演习的结果	12 个月

## 8. 采用的主要技术

### 1) 网络数据流记录

网络信息传输是以流或连接划分的，流是识别、检测、分析网络信息的最小单元。在“爱因斯坦”-1 中，系统监测的数据流记录属性包括自治域号、互联网控制报文协议类型、传输协议、包长度、源地址和目的地址、源端口和目的端口、时间戳、持续时间等；到“爱因斯坦”-2 阶段则采用了更复杂的数据流记录，使得系统可以更深入地剖析传递的信息；“爱因斯坦”-3 保持了与爱因斯坦-2 相同的数据流记录格式。

### 2) 通信指纹

通信指纹是对恶意网络流的特定标记。US-CERT 没有给出通信指纹在“爱因斯坦”系统中的真实定义，但是给出了一个商用的指纹例子作为参考。

“爱因斯坦”-2 对入侵检测的报警是基于已知恶意网络流的通信指纹库。对于随时变化的网络活动元素，现有指纹库仅反映了网络安全事件集的一个子集。

“爱因斯坦”-3 比“爱因斯坦”-2 拥有更丰富的通信指纹库，另外“爱因斯坦”-3 还可对新的网络恶意流实时发现并进行解析，经美国国家安全局与国防部确认后，由国土安全部采用作为新的通信指纹。US-CERT 没有公开的指纹解析方法。显然，通过流解析获取新指纹与现有指纹库互补是“爱因斯坦”-3 的一个亮点。

### 3) 深度包检测（DPI，Deep Packet Inspection）技术

针对五元组的普通包检测技术，已经不足以应付网络威胁。“爱因斯坦”-3 检测的网络流数据属性达到 13 元组，DPI 被作为唯一有效的技术。美国“市场研究传媒”声称：DPI 技术的实施保护了联邦网络；DPI 市场受“爱因斯坦”系统部署的激发而呈爆发式增长。

DPI 深度检测的目的是识别和区分 IP 包的特征和属性。DPI 的“深度”并不是针对每一个 IP 包内检测的长度（字节数），也不是对 IP 包的内容完备地测评，DPI 技术主要指在纵深上对 IP 包分析的能力。这个能力直接反映设备对并发连接的处理能力。因此基于 DPI 技术的“爱因斯坦”-3 系统应具有很强的数据传输能力与计算能力。

### 4) 重定向技术

敏感信息数据流有选择地被重定向是另一个值得关注的技术处理。从网络安全的角度，重定向可以用作主动防御的有效工具。但是，在大规模网络中重定向网络流量并非易事，频繁地修改网络设备的配置会直接地影响整个网络的性能和可靠性。一个较为稳妥并具备可扩展性的方法是在网络的关键节点部署专用设备，透明地转发、镜像、重定向数据流。

### 5) 实时态势感知

“爱因斯坦”-2 探测到特定的网络威胁活动时，提供一定的预判并向 US-CERT 报警，

但它不改变各参与机构自身对网络安全的监控和防御的已有措施。可以认为这种“态势感知”主要是情报的即时共享。

“爱因斯坦”-3 则真正具备了网络态势感知能力。解析未知网络流提取通信指纹的方法弥补了“爱因斯坦”-2 的缺陷,保证了其丰富的通信指纹库;其采用 DPI 技术可实时识别网络的恶意数据流;利用重定向技术,将数据传递给智能系统进行数据深度挖掘分析,并将决策结果反馈给系统以进行处置。

“爱因斯坦”-3 对信息的感知是双向的,当网络流信息进入或离开政府网络时,都进行实时监控。系统利用获取的数据分析相关交叉部门间的网络事件,给联邦政府提供网络活动的高层次视野。“爱因斯坦”-3 还在商用技术基础上增加定制化的功能,并以多部件联动的方式与“爱因斯坦”-2 和“爱因斯坦”-1 互补共存。

可见,强调实时感知处置的、基于 DPI 技术的“爱因斯坦”-3 系统,恰是对 CNCI 的计划 5——“把当前各网络行动中心相互连接,加强态势感知”,从技术层面进行支撑和呼应。

## 9. 使命任务

(1) “爱因斯坦”计划的战略高度。CNCI 反复强调安全防护是在“政府网络”范围,实际却在计划实施细节中列入“增强对各类网络的等级安全防护”。涉及战争、外交、反恐、执法、情报和国土安全等敏感信息的“各类网络”,显然超出了“政府网络”的范畴。

美国国防部从 2000 年开始构建全球信息栅格,作为美国国家安全战略的一个重要支柱。国防部同时也负责“爱因斯坦”系统的研发,因此全球信息栅格也极可能是“爱因斯坦”系统的使用者之一。另外,新成立的美军网络司令部和国土安全部有密切合作,2010 年 5 月上任的首任司令基思·亚历山大曾任国家安全局局长。他在一次公开场合表示,美军必须建立网络通用作战态势图,加强网络实时态势感知能力;军队必须具备实时监控多个计算机网络的能力,以实时响应网络威胁。他还提出对“网上敌人”要实时监控。

(2) “爱因斯坦”-3 计划已部署到公共互联网,美国的政府网络和军事网络实际上由两个部分组成:专用物理隔离网络和租用虚拟隔离网络,虚拟隔离网络就是公共互联网。美国的三大电信运营商——AT&T、Verizon、Sprint 都为美国政府网络和军事网络通信提供支撑和服务。从使用角度来看,已经很难区别政府网络与公共互联网络的界线。“爱因斯坦”-3 演习已经包括了 AT&T 的公共运营网络。

(3) “爱因斯坦”-3 的真实定位。US-CERT 在介绍“爱因斯坦”计划时披露了一些案例界面。例如,美国与全球互联网交互流量按洲际分布的日报,涉及地区包括非洲、亚洲、中美洲、欧洲、北美洲、大洋洲、南美洲,还可呈现日报、月报、年报和时间段、地区的上行/下行数据流量分布、服务端及用户端上行和下行数据流量及协议分布、发生的事件等。这表明“爱因斯坦”系统已经对途经美国的其他网络信息流进行了监控。

当“爱因斯坦”系统在互联网上规模化部署后,就有助于对国际各区域的网络进行态

势感知，从而做到有效的主动防御，甚至先发制人。同时，随着“维基解密”揭秘风波的持续，美国政府就声称将动用“爱因斯坦”系统严密保护政府网络 2400 多个接入点。

由此可见，“爱因斯坦”计划绝不仅仅是联邦政府网络的监管系统，它已经成为美国保卫国家的新一代工具。

### 3.3.6 网络入侵检测系统

#### 1. 入侵检测的概念

入侵检测就是对入侵行为的发觉。它通过对计算机网络或计算机系统中的若干关键点收集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。入侵检测系统（IDS）是实现入侵检测功能的一系列软件、硬件的集合。作为一种安全管理工具，它从不同的系统资源收集信息，分析反映误用或异常行为模式的信息，对检测到的行为做出相应的反应，并报告检测的结果。

#### 2. 入侵检测的作用

具体讲，入侵检测的作用可归结为：①监控、分析用户和系统的非法活动；②核查系统配置和漏洞；③评估关键系统和数据文件的完整性；④识别攻击的活动模式并向网管人员报警；⑤对异常活动的统计分析；⑥操作系统审计跟踪管理，识别违反政策的用户活动；⑦评估重要系统和数据文件的完整性。

#### 3. 入侵检测的工作过程

（1）入侵检测的第一步是信息收集，检测内容包括系统、网络、数据及用户活动的状态和行为。需要在计算机网络系统中的若干不同关键点（不同网段和不同主机）收集信息，这样除了尽可能扩大检测范围的因素外，还有一个重要的因素就是从站点发来的信息有可能看不出疑点，但从几个站点发来的信息的不一致性却是可疑行为或入侵的最好标志。

入侵检测利用的信息一般来自以下四个方面：

第一，系统和网络日志文件。黑客经常在系统日志文件中留下他们的踪迹，因此，充分利用系统和网络日志文件信息是检测入侵的必要条件。日志中包含发生在系统和网络上的不寻常和不期望活动的证据，这些证据可以指出有人正在入侵或已成功入侵了系统。通过查看日志文件，能够发现成功的入侵或入侵企图，并迅速地启动相应的应急响应程序。

第二，目录和文件中的不期望的改变。网络环境中的文件系统包含很多软件和数据文件，包含重要信息的文件和私有数据文件经常是黑客修改或破坏的目标。目录和文件中不期望的改变，特别是那些正常情况下限制访问的，很可能就是一种入侵产生的暗示和信号。黑客经常替换、修改和破坏他们获得访问权的系统上的文件，同时为了隐藏系统中他们的表现及活动痕迹，都会尽力去替换系统程序或修改系统日志文件。

第三，程序执行中的不期望行为。网络系统上的程序执行一般包括操作系统、网络服务、用户启动的程序和特定目的的应用，一个程序的执行出现了不期望的行为可能表明黑客正在入侵你的系统。黑客可能会将程序或服务的运行分解，从而导致程序执行失败，或者以非用户或管理员意图的方式操作。

第四，物理形式的入侵信息。这包括两个方面的内容，一是对未授权的网络硬件进行连接；二是对物理资源的未授权访问。黑客会想方设法去突破网络的周边防卫，如果他们能够在物理上访问内部网，那么他们就能安装自己的设备和软件了。

(2) 入侵检测的第二步是信号分析。对上述四类收集到的有关系统、网络、数据及用户活动的状态和行为等信息，一般通过三种技术手段进行分析：模式匹配、统计分析和完整性分析。其中前两种方法用于实时的入侵检测，而完整性分析则用于事后分析。

第一，模式匹配。模式匹配就是将收集到的信息与已知的网络入侵和系统误用模式数据库进行比较，从而发现违背安全策略的行为。一般来讲，一种进攻模式可以用一个过程（如执行一条指令）或一个输出（如获得权限）来表示。这种方法只需收集相关的数据集合，从而减少了系统负担，目前这种技术已相当成熟。它需要不断地升级来对付不断出现的黑客攻击手法，因为它不能检测到从未出现过的黑客攻击手段。

第二，统计分析。统计分析方法首先给系统对象创建一个统计描述，统计正常使用时的一些测量属性（如访问次数、操作失败次数和延时等）。测量属性的平均值将被用来与网络、系统的行为进行比较，任何观察值在正常值范围之外时，就认为有入侵发生。

第三，完整性分析。完整性分析主要关注某个文件或对象是否被更改，这包括文件和目录的内容及属性，它在发现被更改的应用程序方面特别有效。完整性分析利用强有力的加密机制，它能识别哪怕是微小的变化。其优点是无论模式匹配方法和统计分析方法能否发现入侵，只要是成功的攻击导致了文件或其他对象的任何改变，它都能够发现。缺点是一般以批处理方式实现，不能用于实时响应。尽管如此，完整性检测方法还应该是网络安全产品的必要手段之一。

一般来讲，入侵检测技术根据采用的检测方法可分为两类。

一是异常发现技术。此种技术假定所有入侵行为都是与正常行为不同的。如果建立系统正常行为的轨迹，那么理论上可以把所有与正常轨迹不同的系统状态视为可疑企图。对于异常阈值与特征的选择是异常发现技术的关键。比如，通过流量统计分析将异常时间内的异常网络流量视为可疑。异常发现技术的局限是，并非所有的入侵都表现为异常，而且系统的轨迹难以计算和更新。

二是模式发现技术。此种技术假定所有入侵行为和手段（及其变种）都能够表达为一种模式或特征，那么所有已知的入侵方法都可以用匹配的方法发现。模式发现的关键是如何表达入侵的模式，把真正的入侵与正常行为区分开来。模式发现的优点是误报少，局限是它只能发现已知的攻击，对未知的攻击无能为力。这类方法类似于病毒检测技术，其检测的准确率和效率比较高，大多数入侵检测系统都采用模式发现技术。

#### 4. 入侵检测系统分类

入侵检测系统按其输入数据的来源来看，可以分为基于主机、基于网络、基于代理三

种类型的入侵检测系统。

(1) 基于主机的入侵检测系统，其输入数据来源于系统的审计日志、系统安全日志、应用程序日志等，它把这些审计记录文件与已知攻击模式进行比较，若发现一致，检测系统就发出入侵报警并采取相应的行动，这种入侵检测系统一般只能检测该主机上发生的入侵。

(2) 基于网络的入侵检测系统，其输入数据来源于原始的网络数据包，它实时地监视并分析通过网络传输的通信业务，一旦检测到攻击，入侵检测系统通过报警及中断连接等方式做出反应。它能够检测该网段上发生的网络入侵。

(3) 基于代理的入侵检测系统，即采用上述两种数据来源的分布式入侵检测系统；能够同时分析来自主机系统审计日志和网络数据流的入侵检测系统，一般为分布式结构，由一个中央监视器和多个代理组成，用于监视大型网络系统。

## 5. 入侵检测系统的评价指标

如何评价入侵检测系统，目前尚无规定的评估标准。一般可以从以下几个方面去评价：一是保证自身的安全问题；二是运行与维护系统的开销；三是入侵检测系统报警准确率；四是网络入侵检测系统负载能力，以及可支持的网络类型；五是支持的入侵特征数；六是否支持 IP 碎片重组；七是是否支持 TCP 流重组。

## 6. 入侵检测技术的几个新方向

入侵检测技术有以下几个新的发展方向。

(1) 应用层入侵检测。许多入侵行为只有在应用层才能被确定，现有的入侵检测系统仅仅检测网络层的通信协议，许多基于网络的大型计算机应用系统需要应用层的入侵检测保护。

(2) 通用入侵检测架构。对于异构系统的检测与防护，不同入侵检测系统之间不能协同工作的问题要求开发通用的入侵检测产品。

(3) 智能的入侵检测。随着入侵方法的多样化与综合化，一些入侵检测产品开发商已将一些智能方法应用于产品开发研制，这将很好地解决入侵检测产品的自学与自适应能力。

(4) 全面的安全防御方案。将网络安全作为一个整体工程来处理，从管理、网络结构、病毒防护、防火墙、入侵检测各个方面，全方位地对网络安全做出评估，提出可行解决方案。

### 3.3.7 网络飞机

#### 1. 网络飞机的概念

网络飞机的概念最初是由美国空军研究实验室（AFRL）信息处研究人员 Phister 等人



在其 2004 年发表的文章中提出,此时他们正在研究的一种感知预警类网络武器。它是一种在网络空间域工作的网络平台,执行与常规平台(如无人机)相似的作战任务,如作为“打击”平台(如拒止、摧毁、降级、破坏或欺骗)或“ISR”平台(如发现、定位、跟踪和监视)。其特点为:能从网络平台发射,能在平台内嵌入控制指令,能通过网络进行远程控制,能在经过验证后自我毁灭,能几乎不留痕迹地执行任务,能集结到一起协同工作。

网络飞机主要任务是第一时间侦察到敌方在网络空间内的作战意图,可以在战略级、作战行动级和战术级三个级别发挥作用。在战略级,网络飞机可以执行长期情报收集任务,如收集敌对国家的财务信息、监视其军事部署;在作战行动级,网络飞机可以执行短期的作战行动级任务,如侦察特定区域有多少坦克或装甲车辆、敌方军事领导人身处何方等;而在战术级,网络飞机可以在几分钟到几个小时以内收集实施信息,如敌方坦克在城市内哪个位置。

与物理飞机相比,网络飞机的实质是一种软件,飞行于由各种信息组成的网络空间,并且搭载各种有效载荷,执行短、中、长期的实时信息收集、识别、发送与告警等任务。网络飞机的作战理念非常先进,它由网络战人员进行统一预编程,可以被安装在任何电子介质之中,主动寻找并识别所有软/硬件设备内的网络威胁,并进行告警;如果面对无法识别的威胁,还可以先隔离计算机,再进行下一步的侦察与确认。网络飞机的重要意义在于提供了一种在网络空间内主动防御的作战思想,并且可以保证指挥员对大到整个网络空间、小至任意一台计算机的作战域,都可以进行瞬间感知与控制。专家估计,网络飞机真正投入使用的时间大概在 2020 年前后,并且未来可能会搭载更多的攻击性载荷。

## 2. 侦察手段

目前,类似于网络飞机的侦察预警类武器所携带的有效载荷主要具备以下几种侦察手段:踩点、Ping 扫描、端口扫描、操作系统辨识、漏洞扫描及查点,具体说明见表 3-2。

表 3-2 类似于网络飞机的感知预警类网络武器主要侦察手段

侦察形式	简要描述	典型工具
踩点	正常合法地获取攻击目标信息,全面窥探其安全防御情况	USCAN、CAN-X
Ping 扫描	用以搜寻正在活跃的主机	PingPlus、QuickPing、Icmpenum
端口扫描	与目标主机一些端口建立连接,根据回复确定开放服务情况	ScanPort
操作系统辨识	分析确认目标主机操作系统类型	CheckOS、Nmap、Queso
漏洞扫描	基于漏洞数据库,对目标主机进行扫描,用以发现可利用的安全漏洞	X-Scan、Nessus、Scanner、SuperScan
查点	结合各种技巧和工具,获取目标系统或网络的账号或导出资源名	Ls、NtinfoScan

### 3. 应用想定

一种假想的网络飞机城市作战应用想定如图 3-5 所示。假设一支海军陆战队进入市区，20 分钟前收到情报，队长需要更新信息。于是，他找到一个插座并插入，这个插座让其可以接入城市电力网，进而进入敌方的计算机网络。队长把网络飞机注入系统（图中的  $T_{-1}$ ），其任务是确定叛乱分子和隐蔽军事设施的位置。在时间  $T_0$ ，网络飞机探测到离这支陆战队 300 米以内的一个军事据点有活动。于是，它开始执行侦察任务，收集叛乱分子相关的情报（准确位置、数量、火力配备等），并把收集到的信息发回给陆战队员。但是，这时陆战队员已经移动到了另一个位置，并换用其他方式接入网络。网络飞机感应到该移动并排除干扰因素，重新定位陆战队员新的位置和接口地址。网络飞机捕获到正确的身份信息（ $T_3$ ）并把告警信息发回给陆战队员，告知叛乱分子已经动身，可能正朝他们走来。在时间  $T_N$ ，网络飞机执行其接到的命令（关闭电源，锁上门），发送确认信息并自毁。

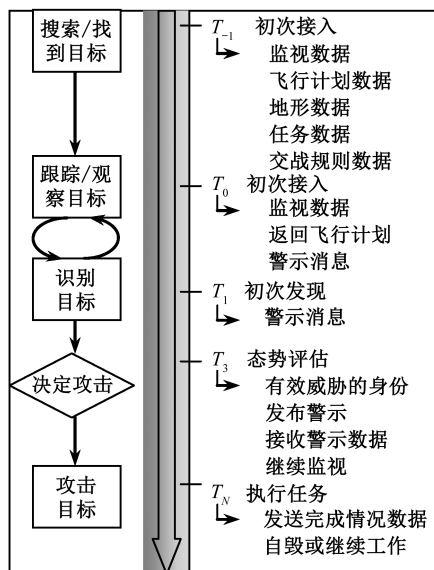


图 3-5 可能的网络飞机城市作战应用想定

上述紧密无缝的行动过程便是网络飞机概念诞生的动因，它彻底颠覆了以往的作战信息的应用理念，把对网络空间作战的认识从以往的计算机攻防，又拉回到具体而又真实的战场。

### 4. 网络飞机的关键技术

美国空军实验室开展网络飞机研究的目的是建立未来的网络飞机接口标准规范，并确保网络飞机是可信任的平台，能够相互协作，为美军提供网络空间优势。

由于网络空间涵盖了整个电磁频谱及其电子信息系统，这里面不仅包含各种信息网络，如互联网、军用信息网络，也包含了涉及其中的电子设备等硬件实体，网络飞机要在

环境如此复杂的网络空间内自由“穿行”和“作战”，美国空军还需要解决很多基本的关键技术问题。

(1) 建立网络空间作战环境模型，构建网络空间作战应用机制。网络空间作战环境远比传统的作战域如陆、海、空、天更加复杂，必须对网络空间作战环境有准确的认知和理解，必须建立准确的网络空间作战环境模型，建立作战视图与作战任务关联性，同时也需要有网络飞机开发环境描述的公用语言，以便对网络飞机获取的数据建立统一的理解。

(2) 解决网络飞机的指挥控制和通信问题。网络飞机具备的“软件”特性决定了对其指挥控制和通信的复杂性，一方面网络飞机的使用会引起国际争议，另一方面网络飞机的潜伏特性决定了对其相关操作要隐蔽进行，甚至不能暴露源头。目前美国空军实验室提出的方案是大规模分布式多级代理系统，但其应用范围仍有待研究。另外，还需要研究代理之间的通信一旦丢失，如何重新建立通信连接相关的问题；如果网络飞机编队分成了几个部分，通信丢失后，一些部分可能会继续收集数据、进行决策和改变与其他部分无关的环境；一旦通信恢复，各部分之间可能会出现数据和策略冲突，因此，要解决如何才能消除这类冲突等问题。

(3) 建立有效的网络飞机状态监控机制。网络飞机的“潜伏”和“软件”特性，使得有些网络飞机可能长期与指挥官失去联系，而在此期间其是否被发现、被破坏或是被利用等潜在风险都对网络飞机状态监控和信任机制提出了很大的挑战，因而需要建立网络飞机形态模型和策略，精确地反映网络飞机的状态变化，确立有效的指挥控制机制和置信度，同时需要开展防篡改/软件保护研究。

(4) 网络飞机很大程度上需要自主运行，面对网络空间这一复杂的作战环境，要想自主运行和作战就需要极高的人工智能水平，这对目前的人工智能技术来说是个很大的挑战。况且，在没能清晰认识和理解网络空间的情况下，要让网络飞机作战这一点就更加困难。

(5) 接口和有效载荷定义研究。需要为网络飞机定义标准接口（如网络飞机与加载平台之间的接口、网络飞机与环境之间的接口，网络飞机与有效载荷之间的接口，网络飞机之间的接口），使其具有可扩展性，成长性和互操作性。网络飞机是网络、加载平台操作系统和有效载荷之间的信息管道，因此这些接口必须很简单且能为代理提供足够的灵活性，以加载新型有效载荷和适应加载平台操作系统的变化。

## 5. 面临的问题

网络飞机的工作环境异常复杂，涉及计算机网络、电子网络、射频网络等，它们既可能是有线网络，也可能是无线网络，如何在这样的环境下无缝穿行；网络飞机代理和有效载荷如何实现；网络飞机如何控制；如何才能不被发现，实现隐身；如何建立必要的信任机制；可以执行哪些作战任务；以及相关作战准则和程序的制定等问题都有待解决。从目前美国空军公布的资料来看，网络飞机的需求定义、信任机制、C3 体系架构，以及作战应用等都有相关论文进行讨论。特别是，由于网络飞机大多数情况下可能需要自主运行，如何确保其运行过程中不被敌方发现、跟踪、控制等，是非常关键的。

### 3.3.8 其他态势感知武器

其他态势感知武器主要有链路数据捕捉系统、传输/数据协议分析系统、情报分析系统、搜索引擎等。例如，百度、谷歌、雅虎、搜狐、搜狗等搜索引擎可以面向作战人员广泛收集信息。从近几年实战情况看，比较有代表性的战场网络侦察设备有美军的“网络中心协同定位（NCCT）”系统、“分析、传播、直观化、深入理解和语言强化”系统，以及“高级侦察员”网络侦察系统。美军的“高级侦察员”网络侦察系统能够寻找对方信息发射源和网络体系入口，具有超高精度的辐射源测向、定位和语音识别能力，可由 EC—130H 战术运输机、U—2 高空侦察机和“全球鹰”高空无人机携带。

## 3.4 网络空间进攻武器

### 3.4.1 网络空间进攻武器的分类

网络空间进攻主要是通过信息的收集、分析、整理以后，发现目标系统的弱点，有针对性地目标系统（服务器、网络设备与安全设备）进行资源入侵与破坏、机密信息窃取、监视和控制。

网络空间进攻武器主要执行网络进攻任务，按照作战手段的不同，可分为“软进攻”与“硬进攻”两类武器。

#### 1. “软攻击”类网络武器

“软攻击”类网络武器并不具备物理实体，主要包括窃听、欺骗、拒绝服务、数据驱动、隐藏、综合等。

（1）窃听类武器。主要利用观察、记录、监听、访问等非法手段，窃取敌方各种关键信息。目前，窃听类武器的攻击形式包括键盘记录、网络嗅探、非法访问、密码盗取等，典型工具包括 Infostealer、Sniffer Pro、Passware Kit 等。

（2）欺骗类武器。可冒充正常用户访问敌方系统或网络，进而获取信息资源，主要包括口令获取、恶意代码、网络欺骗等攻击手段。像各种木马程序、邮件病毒、网页病毒等都属于恶意代码；而 IP 欺骗、邮件欺骗、会话劫持、选路信息协议（RIP，Route Information Protocol）路由欺骗、地址解析协议（ARP，Address Resolution Protocol）重定向等都属于网络欺骗。目前，典型欺骗类工具有 John the Ripper、Nimda、Trojan Horse、IPMap、Juggernaut、Duqu 等。Duqu 是一种复杂的木马，其主要功能是充当系统后门，窃取隐私。

Duqu 架构所使用的语言高度专业化,能够让设计极限载荷(DLL, Design Limit Load)同其他 Duqu 模块独立,通过多种途径包括 Windows HTTP、网络端口和代理服务器同 C&C 建立连接。还能够让 DLL 直接处理来自命令与控制(C&C, Command and Control)的超文本传输协议(HTTP, HyperText Transfer Protocol)服务器请求,甚至可以在网络中的其他计算机上传播辅助恶意代码,实现可控制并且隐蔽的感染手段,殃及其他计算机。

(3) 拒绝服务类武器。拒绝服务(DoS, Denial of Service)是网络作战人员的终极手段。它利用超出目标处理能力的海量数据包消耗目标的主机、网络带宽、信息资源,致使对方无法使用任何服务,其攻击形式包括资源耗尽与导致异常两种。分布式拒绝服务(DDoS, Distributed Denial of Service)攻击是在 DoS 的基础上发展起来的资源耗尽型攻击技术。

(4) 数据驱动类武器。通过向目标发送数据导致非预期攻击结果的产生,主要包括缓冲区溢出、格式化字符串、输入验证、同步漏洞、信任漏洞等攻击样式,近年来比较著名的蠕虫均属于缓冲区溢出类型。目前典型的数据驱动类工具有 Code Red、Blaster 等。

(5) 隐藏类武器。用来消除网络攻击过程留下的痕迹,并且为日后继续侦察或攻击留下轻易进入的快速通道,主要包括日志清除、后门安装以及内核控制等攻击形式,典型工具包括 Clearlogs、ZAP、Knark 等。

(6) 综合类武器。具有窃听、攻击、运载等多种功能的软攻击网络武器。典型的有僵尸网络(Botnet)、火焰病毒等。

实际上,僵尸网络属于各种“软攻击”类网络武器的运载系统,类似于投送卫星的运载火箭,它利用一种或多种手段向大量主机传播僵尸程序,进而在攻击者和被感染主机之间形成一种一对多的控制网络,恶意控制此网络内所有主机,最终利用这些主机发动上述提到的各种“软攻击”。其中,主体功能模块实现本体功能,辅助功能模块实现其他的辅助功能(攻击、防御、分析、维护等)。目前,比较典型的包括因特网中继聊天(IRC, Internet Relay Chat)僵尸网络(如 Sdbot、Agobot 等)、HTTP 僵尸网络(如 Bobax、Rustock 等)及对等的(P2P, Peer-to-Peer)僵尸网络(如 Phatbot 等)。

火焰病毒是一种复杂的攻击工具,远比 Duqu 的结构复杂。它既是一种后门程序、木马,却又具有蠕虫的特点,只要其背后的操控者发出指令,它能够在本地网络、移动设备中进行自我复制,能够记录来自内部话筒音频数据,能够操控蓝牙设备的使用。

Flame 是一个庞大的程序包,全部部署的话,大约有 20MB。包含了很多不同的功能,诸如压缩(zlib、libbz2、PPMD)和数据库操控(SQLite3),同时还要一个 Lua 虚拟设备,还有含嵌套结构化查询语言(SQL, Structured Query Language)请求的内部数据库、多个加密方法、多重加密运算法则,使用 Windows Management Instrumentation 大量编写脚本及进行其他操作。

## 2. “硬攻击”类网络武器

该类网络武器主要是指定向能武器等真实存在的物理作战实体,主要包括激光武器、射频武器和粒子束武器三种类型。定向能武器利用高热、电离、辐射等效应,将能量聚集

形成高能强束流，实现干扰或损坏敌方电子信息系统，甚至造成人员伤亡的作战目的。高功率微波武器是目前比较流行的一种定向能武器，它主要由初始能源、激励电源、高功率微波发生器、发射天线和其他辅助设备组成。在工作时，高功率微波武器首先利用高功率微波发生器将电子束的动能转换成强电磁能量，然后以极窄的脉冲通过高增益天线形成一个强大的微波束定向辐射，最后经由电子信息系统的前门（对外开放的通道，如天线）进入而形成攻击效果。

### 3.4.2 常用的网络空间进攻武器

目前世界上有 17 种常见的网络空间进攻武器，下面一一加以简单介绍。

#### 1. 软件漏洞

软件漏洞是由于软件开发者的疏忽，或者软件开发所使用的语言的局限性，甚至软件错误代码或软件本身错误所造成的，使得软件在使用的过程中软件自身存在缺陷和弱点。漏洞往往是病毒木马入侵计算机的突破口，这些有缺陷的程序容易让一些软件高手找出并进行软件内部的破解与破坏。如果掌握了漏洞的技术细节，能够研究漏洞如何被利用，往往可以让目标主机执行任意代码。这仍然是目前最常见和最危险的网络攻击手段。

#### 2. 计算机病毒

计算机病毒是编制者在计算机程序中插入的破坏计算机功能或数据的代码，或依附于其他软件的恶意程序，能影响计算机的使用，能自我复制的一组计算机指令或程序代码。它能潜伏在计算机的存储介质（或程序）里，甚至伪装成合法的软件补丁，条件满足时即被激活，通过修改其他程序的方法将自己精确复制或者可能演化的形式放入其他程序中。从而感染其他程序，对计算机资源进行破坏。就像生物病毒一样，具有自我繁殖、互相传染以及激活、再生等生物病毒特征。计算机病毒有独特的复制能力，它们能够快速蔓延，又常常难以根除。它们能把自身附着在各种类型的文件上，当文件被复制或从一个用户传送到另一个用户时，它们就随同文件一起蔓延开来。

计算机病毒具有传播性、隐蔽性、感染性、潜伏性、可激发性、表现性或破坏性。计算机病毒的生命周期：开发期→传染期→潜伏期→发作期→发现期→消化期→消亡期。

#### 3. 内部植入威胁

内部植入威胁是一种比较原始但威胁很大的手段，通过向对方基地渗透人员，见机向网络注入恶意病毒或代码。在对方网络被物理隔绝的情况下，这种方式非常有效。据称，以色列为袭击伊朗核设施，曾派特工潜入伊朗，通过 U 盘向核设施网络植入病毒。

## 4. 逻辑炸弹

逻辑炸弹是指在满足特定条件（如特定指令、特定日期和时间）时，对目标系统实施破坏的计算机程序。如修改、冲掉信息数据，释放病毒，抑制系统功能的发挥，计算机不能从硬盘或软盘引导，造成系统混乱，甚至会使整个系统瘫痪，并出现物理损坏的虚假现象。其中，在特定时间发作的逻辑炸弹称为时间逻辑炸弹，在特定事件产生中发作的逻辑炸弹称为事件逻辑炸弹。如果把计算机病毒看成是飞行中的导弹，而逻辑炸弹就是待发射的导弹或定时炸弹。一旦某个逻辑诱因满足，逻辑炸弹随时可能对用户造成无法预知的后果。

多数可用于军事目的的设备中，如大型计算机、程控交换机等，都可能有逻辑炸弹。在这些设备中安装逻辑炸弹是为了窃取国家和军队的机密信息，或者在某些关键时刻，使国家和军队的指挥控制系统崩溃。例如，某个国家在出口敏感性很强的计算机系统时，出于本国未来安全战略的考虑，可在软件系统中预先隐藏设置逻辑炸弹，一旦出现关系紧张或敌对危机时，从外部引发逻辑炸弹，为本国军事目的服务。

## 5. 特洛伊木马

黑客的主要攻击武器之一，就是采用特洛伊木马技术，渗透到对方的主机系统里，从而远程操作目标主机，偷窃计算机中的文件和数据，窃取你的口令，浏览你的驱动器，修改你的文件，登录注册表等。

特洛伊木马（以下简称“木马”）是一种基于远程控制的黑客工具。通过互联网资源隐蔽地对远程目标主机进行非授权的访问。木马对系统具有强大的控制功能，操纵木马的人可以通过网络像使用自己的机器一样远程控制木马所在的目标主机，甚至可以远程监控受控主机上的所有操作。

完整的木马程序一般由两个部分组成：一个是服务器程序，一个是控制器程序。中了木马就是指被安装了木马的服务器程序。若你的计算机被安装了服务器程序，则拥有控制器程序的人就可以通过网络控制你的计算机而为所欲为，这时你计算机上的各种文件、程序，以及在你计算机上使用的账号、密码就无安全可言了。

## 6. 隧道攻击

隧道是一种封装，即把一种协议的报文封装在另一种协议的报文中进行传输。通过使用隧道，可以轻易地突破防火墙，从而实现远程控制。通过获取底层系统功能而在安全系统的更低层发动攻击，比如利用计算机防火墙本身的缺陷侵入系统。

## 7. 后门程序

后门是一种登录系统的方法，它不仅绕过系统已有的安全设置，而且还能挫败系统上各种增强的安全设置。后门程序是程序软件开发者或系统研制者有意设计并隐藏在计算机程序中的几段特定程序。隐藏的目的就是给设计者留有后门，程序可根据设计者的需要随

时激活，并使设计者能通过后门随时突破系统的安全保护措施，就如同使用自己的计算机系统一样，非法侵入并获得允许权限外的信息。如某个国家在出口计算机系统时预先埋藏计算机“陷阱”，根据本国网络空间作战、军事战略仿真或情报等目的通过“后门”进出对方敏感系统，窃取重要信息。比如，可以利用后门在程序中建立隐藏通道，甚至植入一些隐藏的病毒程序等。利用后门可以使原来相互隔离的网络信息形成某种隐蔽的关联，进而可以非法访问网络，达到窃取、更改、伪造和破坏信息的目的，甚至有可能造成网络信息系统大面积瘫痪。例如，国外很多厂家的路由器都具有一种远程维护功能，即可以通过远程终端，由公开预留的接口（如路由器的远程登录超级口令）进入系统完成维护检测功能。这种功能在带来维护管理便利的同时，当然也带来了一种潜在的威胁。

后门程序与木马有联系也有区别。联系在于：后门程序和木马都是隐藏在用户系统中向外发送信息，而且本身具有一定权限，以便远程机器对本机的控制。区别在于：木马是一个完整的软件，而后门程序则体积较小且功能都很单一。后门程序类似木马，其用途在于潜伏在计算机中，从事收集信息或便于黑客进入的动作。后门程序和计算机病毒最大的区别在于：后门程序不一定有自我复制的动作，也就是后门程序不一定会“感染”其他计算机。

## 8. 蠕虫病毒

在受感染计算机中植入蠕虫病毒，逐一扫描 IP 地址，确定主机是否在活动、主机正在使用哪些端口、提供哪些服务，以便制订相应的攻击方案。

蠕虫病毒是一种专门针对网络而设计的恶意程序。它通过网络的通信设施蠕动、扭动和爬行，在此过程中传播并影响信息和信息系统。蠕虫病毒传播速度快，可以造成任何种类的破坏。但蠕虫病毒无繁殖再生功能，不像计算机病毒那样修改其他程序，而是修改文件、侵占存储空间、侵蚀资源、替换或冲掉有价值的信息，造成信息数据的丢失。

## 9. 字典式扫描

扫描中的字典是暴力破解密码用的，一般字典文件里包含大量的所有可能被目标使用的字符串，破解时字典会在字典文件中顺序抽取字符串进行密码配对。扫描器是一种自动检测远程或本地主机安全性弱点的程序。字典式扫描就是利用目标客户端的缓冲溢出弱点，取得计算机的控制权。

实施一次字典扫描攻击需要具备两个要素：要素一是进攻方了解认证方式（包括认证协议以及地址、端口等信息），如同小偷需要知道库房在哪儿，房门挂着的是大铜锁还是密码锁，甚至虹膜、指纹识别；要素二是进攻方拥有比较全面的口令集，包含着各类常见的弱口令，或者目标系统经常出现的组合口令，或者目标系统曾经泄露的口令集。这样才有更多的尝试机会。通常一次字典扫描进攻的实施还是很耗费时间的，特别是目标系统的口令不那么常见的。



## 10. 数字扫描

数字扫描主要跟踪和刺探网络用户的行踪，以获取密码或其他数据，主要用于对无线局域网的攻击。

## 11. 数据回收

数据回收主要收集废弃存储介质，还原大量未受保护的数据，获取相应系统的漏洞线索。

## 12. 僵尸网络

僵尸网络是由感染了特定恶意代码的大量受害主机组成并被攻击者远程控制的网络，这是一种隐匿、复杂、灵活、高效的网络攻击平台，在互联网中分布非常广泛。攻击者通过一对多的命令与控制信道，控制大量主机，采用各种传播手段，将大量网络主机感染僵尸程序，恶意控制此网络内所有主机，众多的计算机在不知不觉中如同僵尸群一样被人驱赶和指挥，成为被人利用的一种工具。僵尸网络使攻击者具备了实施大规模恶意活动的能力，利用僵尸网络，攻击者可以轻易地控制成千上万台主机对因特网任意站点发起分布式拒绝服务攻击，并发送大量垃圾邮件、木马和间谍软件，从受控主机上窃取敏感信息或进行点击欺诈以牟取经济利益。全球有将近 15% 的在线计算机属于僵尸网络的一部分。

僵尸网络是从传统恶意代码形态包括计算机病毒、网络蠕虫、特洛伊木马和后门工具的基础上进化，并通过相互融合发展而成的目前最为复杂的攻击方式之一。一个僵尸网络可以控制大量的用户终端，可以获得强大的分布式计算能力和丰富的信息资源储备。僵尸网络是一种控制命令驱动的信息系统，它的行为取决于控制者的命令输入。因此，一个具体的僵尸网络可能造成的危害通常难以预测。从已有的僵尸网络来看，其危害已影响到政治、经济和国家安全等多个重要领域，其对军事领域的影响更是凸显。

按照网络结构的划分，僵尸网络可分为单服务器星形结构、多服务器结构、层次结构和随机结构 4 种类型，也有人分为中心式、非中心式和机动式 3 种；根据是否附着在其他网络上，僵尸网络还可以分为自生式和寄生式两种；按照命令与控制信息传递的方式，僵尸网络也分为推送式和拉取式两种类型。

僵尸网络的功能结构如图 3-6 所示。其中，主体功能模块实现本体功能，辅助功能模块实现其他的辅助功能（如攻击、防御、分析、维护等）。目前，比较典型的包括 IRC 僵尸网络、HTTP 僵尸网络及 P2P 僵尸网络。

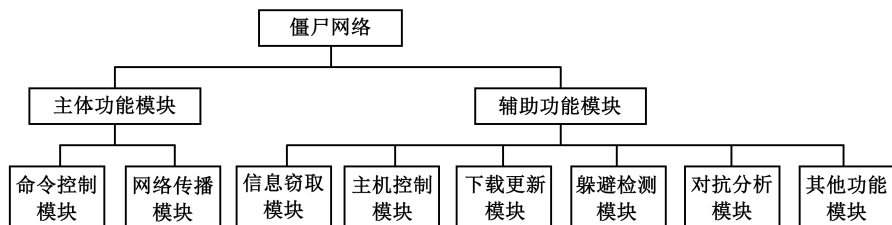


图 3-6 僵尸网络的功能结构

### 13. 电磁脉冲武器

电磁脉冲武器是一种正在发展中的新概念武器，它是利用核爆炸或高能微波发生器产生的强大电磁脉冲，硬摧毁计算机网络系统中的各种电子元器件，包括微处理器、内存、网络设备的芯片等，进而在物理上对网络实施破坏，使整个网络系统陷入瘫痪。美国等国家正在加紧研制试验这种武器，一旦研究成功，就有可能成为未来使用最广且最具威力的武器。

电磁脉冲武器威力巨大，能在短时间内释放巨大能量（百万分之一秒内产生 12 万伏电压和 1000 万安培电流，生成万亿瓦级的功率流）、杀伤频率范围广（影响频率覆盖超低频到超高频），以及投放方式多（导弹、飞机、火炮发射或人工携带）等特性，使其能够对大范围内一切正在使用的军用和民用网络系统造成损害，不仅使敌方军队的指挥控制系统陷入崩溃，而且可以破坏普通民众的正常生产和生活，从而影响敌国指挥当局战略决策。

### 14. 细菌病毒

细菌病毒感染计算机操作系统，通过不断地自我复制使计算机中央处理器瘫痪。

### 15. 欺骗式攻击

欺骗的原理就是冒充身份，就是攻击者伪装成网段里的某一台主机，从而获取其他主机与被攻击者的通信数据。也就是说，欺骗式攻击就是冒充正常用户访问敌方系统或网络，进而获取信息资源，主要包括口令获取、恶意代码、网络欺骗等攻击手段。其中，恶意代码与网络欺骗尤其受到网络作战人员的青睐，像各种木马程序、邮件病毒、网页病毒等都属于恶意代码。欺骗的主要方式有 IP 欺骗、ARP 欺骗、域名系统（DNS，Domain Name System）欺骗、Web 欺骗、电子邮件欺骗、源路由欺骗（通过指定路由，以假冒身份与其他主机进行合法通信或发送假报文，使受攻击主机出现错误动作）、地址欺骗（包括伪造源地址和中间站点）等。目前典型欺骗类工具有 John the Ripper、Nimda、Trojan Horse、IPMap 和 Juggernaut 等。

### 16. 拒绝服务（DoS）/分布式拒绝服务（DDoS）

DoS/DDoS 是目前应用范围最广的网络武器，不过其威胁指数只有 2.9。DoS 攻击手段侧重于向受害主机发送大量看似合法的网络包，DDoS 与 DoS 攻击机理类似，只是采用很多台计算机作为向目标发送信息的攻击源头，从而使目标系统更加难以防范。

DoS 利用超出目标处理能力的海量数据包消耗目标的主机、网络带宽、信息资源，致使对方无法使用任何服务，这是黑客常用的攻击手段之一，其攻击形式包括资源耗尽与导致异常两种。其实对网络带宽进行的消耗性攻击只是 DoS 攻击的一小部分，只要能够对目标造成麻烦，使某些服务被暂停甚至主机死机，都属于 DoS 攻击。DoS 攻击问题一直得不到合理的解决，究其原因是由于网络协议本身的安全缺陷造成的，从而 DoS 攻击也成了攻击者的终极手法。攻击者进行 DoS 攻击，实际上让服务器实现两种效果：一是迫使服务器的缓冲区满，不接收新的请求；二是使用 IP 欺骗，迫使服务器把合法用户连接复位，

影响合法用户的连接。

DDoS 攻击是在 DoS 的基础上发展起来的资源耗尽型攻击技术。DDoS 攻击指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动 DDOS 攻击，从而成倍地提高拒绝服务攻击的威力。通常，攻击者使用一个偷窃账号将 DDOS 主控程序安装在一个计算机上，在一个设定的时间主控程序将与大量代理程序通信，代理程序已经被安装在网络上的许多计算机上。代理程序收到指令时就发动攻击。利用客户/服务器技术，主控程序能在几秒钟内激活成百上千次代理程序的运行。相较于一对一的 DoS 攻击，DDoS 则更难以防范，被称为洪水攻击，其基本原理如图 3-7 所示。DDOS 是利用更多的傀儡机来发起进攻，因此产生的攻击效果更为强大。另外，由于攻击者是通过控制傀儡机传达攻击命令，而不是直接去控制攻击傀儡机，因此难以被追查。典型的 DoS 工具有 Trinoo、TFN 和 Teardrop 等。

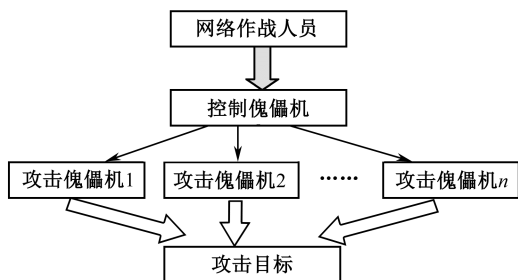


图 3-7 DDoS 基本原理

## 17. 野兔病毒

野兔病毒通过不断自我复制耗尽有限的计算机资源，但并不会感染其他系统。

《网络武器威胁矩阵报告》列出了上述 17 种网络攻击武器在 2004 年、2006 年、2008 年和 2010 年的威胁指数，此外还给出了检测难度、目前可用性和使用率系数，详细内容见表 3-3。

表 3-3 网络武器威胁矩阵

威胁手段	2004 年	2006 年	2008 年	2010 年	检测难度	目前可用性	目前使用率
软件漏洞	3.0	3.7	4.2	3.9	4.0	4.0	4.6
计算机病毒	3.5	3.8	4.1	3.8	3.0	4.0	4.5
内部植入威胁	3.0	3.5	3.8	3.7	4.0	3.5	4.3
逻辑炸弹	3.5	3.8	4.1	3.7	3.7	4.0	3.2
特洛伊木马	3.0	3.5	3.8	3.7	4.0	3.5	4.3
隧道攻击	2.9	3.4	3.9	3.5	3.2	3.5	3.8
后门程序	3.0	3.2	3.5	3.5	4.5	3.0	3.5
蠕虫病毒	3.1	3.5	4.1	3.5	3.2	3.2	3.7

续表							
威胁手段	2004 年	2006 年	2008 年	2010 年	检测难度	目前可用性	目前使用率
字典式扫描	2.9	3.4	4.0	3.4	3.2	3.5	3.6
数字扫描	1.8	2.6	4.0	3.3	3.8	3.8	3.7
数据回收	2.9	3.3	3.9	3.3	2.5	3.0	2.3
僵尸网络	3.0	3.3	3.9	3.0	2.5	3.0	2.3
电磁脉冲武器	2.2	3.5	3.8	3.0	3.8	3.2	1.5
细菌病毒	3.0	3.3	3.9	3.0	2.5	3.0	2.3
欺骗式攻击	3.3	3.5	3.8	3.0	3.0	2.4	2.0
拒绝服务	1.9	2.9	4.1	2.9	1.0	4.1	3.5
野兔病毒	3.0	3.1	3.1	2.8	2.5	3.0	2.3

17 种网络攻击武器，威胁指数最高为 4.1，最低为 1.8。其中，威胁指数在 3.0 以下的为低风险威胁，指数在 3.2~3.4 的是中等威胁，指数为 3.5 以上的是高风险威胁。

### 3.4.3 舒特系统武器

运用网络侦察、入侵、窃取、控制、反制、欺骗、瓦解、降级、破坏、攻击等方式，可能改变武器的机械能、电磁能、化学能的释放强度和释放目标，变硬杀伤、硬摧毁为软杀伤、软瘫痪、软致盲，达到特定的战争威慑和作战效果。其中，舒特系统已经在入侵、窃取、注入、控制等方面取得了很大成功。

#### 1. 舒特系统研制计划的来由

舒特（Suter）系统研制计划是美国空军为弥补对敌防空压制能力的不足而提出的。舒特的名称来自美国“红旗”演习创立者——理查德·穆迪·舒特上校。舒特系统研制计划从 20 世纪 90 年代启动，承包商为 BAE 系统公司。2001 年 7 月，美国国防部呈交国会的《网络中心战》报告（附件）中首次正式披露了舒特系统相关情况。2002 年 11 月，美国《航空周刊和空间技术》杂志中的一篇报道首次向世人揭示了舒特系统的存在。

事实上，舒特系统研制计划从 2000 年开始实施后，就采取了渐进式推进方法，2 年为一个周期，陆续发展了“舒特-1”至“舒特-5”。其中“舒特-1”“舒特-2”“舒特-3”“舒特-5”参加了 2000 年、2002 年、2004 年、2008 年的“联合远征部队试验”，“舒特-4”参加了 2006 年的“红旗”军演。

#### 2. 基本概念

舒特系统是一个空基网络攻击系统，旨在用于战场网络环境中入侵、欺骗，甚至接管敌方的综合防空电子系统。舒特系统实际上采用了一种集战场侦察、电子干扰、网络攻击、精确打击于一体的综合性攻击技术，可以通过敌方雷达天线、微波中继站、网络处理节点

侵入敌方防空网络系统。舒特系统具有自动定位、目标瞄准、(无线)入口扫描、数据注入(病毒、软件算法包等)、网络攻击、雷达预警和可硬摧毁等协同功能。目前,各组织和研究机构对舒特攻击行动的组成要素、主要任务、重要活动,以及交互关系等问题已经有了清晰的认识。

典型的舒特机载网络攻击系统由 RC—135U/V/W 电子侦察飞机、EC—130H 专用电子战飞机或 EA—6B 等普通电子干扰飞机和 F—16CJ 战斗机组成。其中,电子侦察飞机负责信息获取,电子战飞机主要负责对敌方信息系统进行软打击,包括电子干扰和恶意信息输入等,而战斗机则负责对敌方信息系统进行硬打击,从实体上进行摧毁。

据报道,2007年9月6日晚,以色列18架F—16I非隐身战斗机突破俄制“道尔—M1”导弹防御系统,成功轰炸了位于土叙边境的疑似核设施建筑,并成功从原路返回,整个过程完全未被叙利亚防空系统发现。“道尔—M1”系统采用三坐标雷达控制,被称为“具有先进雷达性能、抗干扰能力和目标识别能力的世界一流的防空系统”。此次行动以军使用了美军的舒特技术,成功侵入叙军防空雷达网,“接管”其控制权,使之完全处于失效状态。

舒特正在小型化,向隐身无人机和作战飞机上改装。目前,美国F—22、F—35、EA—18G和F/A—18E/F等新型战机,都携带了新型、远程、有源电扫描阵列,具有部分电子攻击和网络入侵功能,以更好地适应网络/电子攻击任务。其中,一些类似舒特的网络入侵功能,还准备安装到高功率微波导弹、MALD—J干扰型导弹,以及能执行电子攻击任务的MK82系列炸弹上。

### 3. 舒特系统攻击原理

军事网络中大量无线技术的使用,使得薄弱环节越来越多,渗入敌防空系统网络就需要通过无线传感器、无线通信系统、无线通信链路、无线中继链路等途径进入信息处理设备和网络节点。舒特系统正是以敌方电子信息系统中薄弱的雷达、通信系统的天线为入口,渗透进入敌方的防空网,实施网络攻击。装备舒特系统的飞机至少要加装“长矛”吊舱和“豹穴”软件。其中,“长矛”吊舱是一种功率强大的专用辐射源阵列,“豹穴”软件则是一种实施网络入侵的算法/程序。这样,实施攻击时,就能通过“长矛”吊舱发射大功率信号,渗透进敌方网络,然后根据具体攻击战术,采取以下措施:产生假目标;引导雷达在错误方向上搜索;用假目标或信息“淹没”其系统;迫使其系统转换工作模式;植入算法软件包,控制其网络并操纵其雷达转动。

### 4. 舒特攻击的目标

美国研制舒特系统的主要目的就是情报、监视与侦察与进攻性信息战和进攻性空中作战打击平台进行横向一体化集成,实现侦察、情报与软硬打击手段全面结合,使美国空军具备让敌方防空预警系统丧失作战能力。在实际运用中,舒特系统利用敌方雷达、微波中继站和网络处理节点侵入敌方防空计算机网络系统,注入欺骗信息和处理算法,实时监控敌方防空预警雷达的探测结果,或者在此基础上以系统管理员身份接管敌方网络,实现对传感器(主要是雷达)的控制,从而物理操作敌方的传感器。

舒特攻击的目标按攻击阶段可以分为 4 类：设备目标、系统目标、网络目标和时敏目标。设备目标是指构成敌方联合防空系统的基础性硬件，如雷达、天线、中继器、信息处理设备；系统目标是指构成敌方联合防空系统的应用系统，如数据处理系统、计算机系统、通信系统、指挥控制系统等；网络目标是指连通设备和各应用系统的有线或无线网络及其设施，如网络处理节点、通信链路、中继链路等；时敏目标是指必须在有限的“攻击窗口”或“交战机会”内发现、定位、识别、瞄准和攻击的目标，一般可分为两类：各类飞行器和地面活动目标（如战术弹道导弹发射架）。

## 5. 舒特攻击的步骤

在实施舒特攻击的整个过程中，需要侦察监视、网络攻击、电子攻击和常规攻击密切协同，共同来完成任务，具体可概括为以下三步。

第一步，对目标实施电子侦察。使用 RC—135U/V/W 电子侦察飞机在敌方防空区外进行信号和信息侦察，及时掌握敌方防空体系的无线电联络内容。如果遇到不能实时破译的密码，可以立即通过全球信息系统送到美国国家安全局，对侦收到的各类信号参数和信息进行分析、识别、处理，然后将有关信息传递给地面指控中心。

第二步，根据作战目的选择攻击方式。舒特机载网络攻击系统可选择的攻击方式有 3 种：①通过数据链路将目标信息传递给 EA—6B、EA—18G 等电子战飞机，由它们对预定目标实施电子干扰；②通过数据链路将目标信息传递给 F—16CJ 或其他战斗机，由它们对预定目标实施反辐射攻击或精确火力打击；③通过数据链路将目标信息传递给 EC—130H 专用电子战飞机，由其对预定目标实施网络战攻击。

第三步，实施网络攻击。当地面指控中心决定以 EC—130H 专用电子战飞机对预定目标实施网络战攻击时，首先由 RC—135U/V/W 电子侦察飞机通过网络中心目标瞄准系统对敌方辐射源进行高精度定位，然后由 EC—130H 专用电子战飞机向敌方雷达或通信系统的天线发射电子脉冲信号。与传统电子干扰或电磁脉冲攻击不同的是，这些电子脉冲流不是使用过载的“噪声”或能量淹没敌方的电子设备，而是向敌方脆弱的处理节点植入定制的信号，包括专业算法和恶意程序，或巧妙渗入敌方防空雷达网络，或窥测敌方雷达屏幕信息，或实施干扰和欺骗，或冒充敌方网络管理员身份接管系统，从而操纵雷达天线转向，使其无法发现来袭目标。

## 6. 舒特系统攻击方式

依靠舒特系统，网络进攻一方无须通过人工在敌方通信光缆、电缆上搭线，无须人员接近对方设备，也无须通过间谍等情报人员打入敌方内部用人工的手段往目标网络植入病毒或插入其他零部件。在“凭空”进入目标网络完成遥侵之后，舒特网络攻击系统还能实现“遥控”敌方网络的目标。

（1）远程无线入侵。舒特系统能使操作员进入敌方防空系统计算机网络，甚至让操作员作为对方系统管理员，控制网络和操纵敌方雷达传感器。舒特技术能入侵敌方敏感目标跟踪链路，如移动式地空导弹发射台。舒特系统包含一些用来大量检测各类电子发射信号的高效能传感器，它的计算机软件能识别敌方发射机数据库的数据。这个过程包括确定敌

方发射台的准确位置, 导入多个虚假目标的数据流, 以及误导许多活动信息。

(2) “以网制网”对抗。舒特系统对信息网络的攻击采用“无线侵入”的方式实施“网络攻击”。在用电磁波干扰正常通信的同时, 以网络攻击植入“木马”病毒瘫痪敌方指挥控制系统, 或伪造管理员身份发布虚假信息影响指挥员决策、作战部署等。其目的是利用舒特系统优势开展“以网制网”的对抗, 实现作战效果最大化。

(3) 微创介入打击。舒特机载网络攻击系统, 使打击像微创手术一样依靠先进的介入技术, 实现无形空间和有形空间双重精确作战。其实质是首先依靠信息技术渗透进入敌作战网络的要害部位进行控制或瘫痪, 同时以精确作战力量对其体系要点实施破坏袭击。

(4) 电子传感控制。舒特系统具备对监视、预警探测系统的致盲、致瘫能力。一般采取以下3种方法侵入系统: 一是在传感器内部的无线通信数据中植入控制指令或“木马”病毒, 破坏数据处理系统; 二是将控制指令或“木马”病毒植入传感器探测回传数据中, 破坏对方的探测控制系统; 三是在监视、预警和通信卫星通信数据链中插入大量虚假信息, 干扰正常的监视、预警、通信行为, 降低卫星监视、预警和通信能力。

## 7. 舒特攻击行动过程分析与建模

舒特攻击行动从行动过程和任务角度划分, 可以分为3个阶段12个行动。3个阶段为攻击筹划阶段、综合攻击阶段和纵深攻击阶段(或称攻击生效阶段)(与舒特攻击的3个步骤相对应)。舒特攻击过程的建模是基于统一建模语言(UML, Unified Modeling Language)活动图的方法进行, 其模型如图3-8所示。活动图是UML状态图的变体, 可理解为传统意义上的流程图, 主要用于描述系统的动态行为。

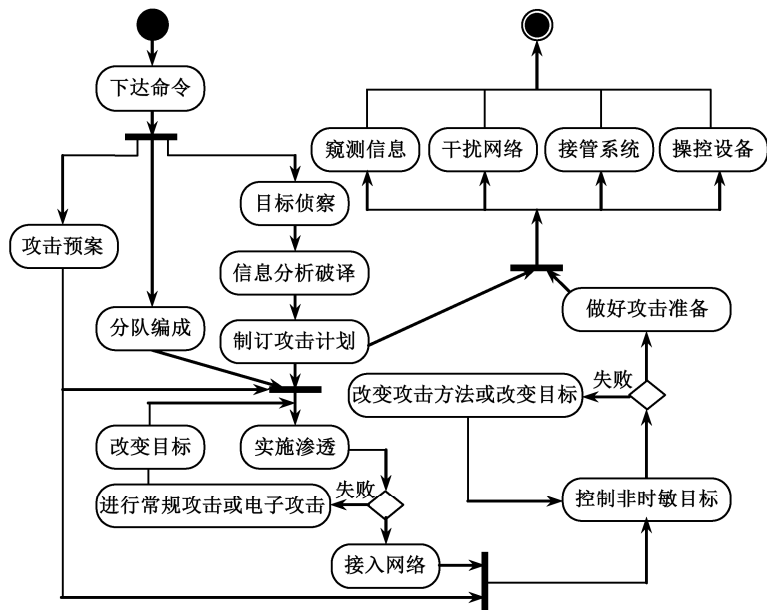


图 3-8 舒特攻击过程模型

## 8. 舒特系统的评价指标

舒特攻击行动效能评估指标体系层次结构如图 3-9 所示。

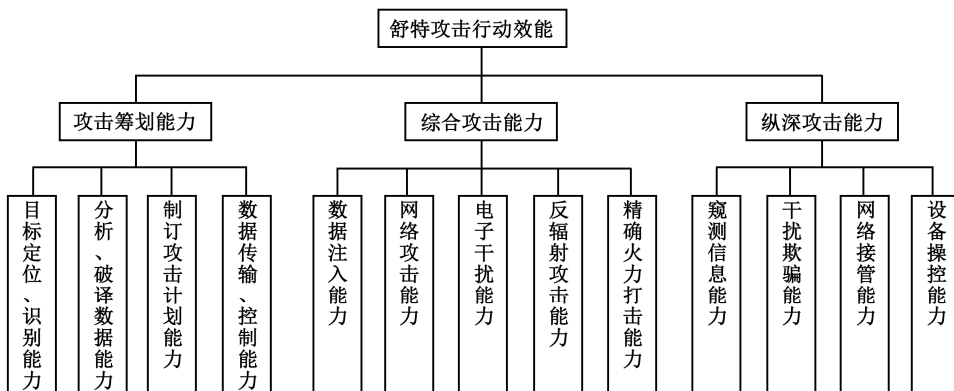


图 3-9 舒特攻击行动效能评估指标体系层次结构

由图 3-9 可以得出，攻击筹划能力、综合攻击能力、纵深攻击能力构成了属性指标，它们反映了舒特攻击行动的基本能力。攻击筹划能力是攻击发起者实施攻击前确定目标、处理数据和制订计划的能力，主要包括目标定位、识别能力，分析、破译数据能力，制订攻击计划能力和数据传输、控制能力；综合攻击能力是综合各种攻击方式对重要目标进行攻击和侵入的能力，目的是秘密侵入目标网络系统内部，主要包括数据注入能力、网络攻击能力、电子干扰能力、反辐射攻击能力和精确火力打击能力；纵深攻击能力是攻击者成功侵入目标网络系统后进一步实施攻击活动的的能力，主要包括窥测信息能力、干扰欺骗能力、网络接管能力和设备操控能力等。

舒特系统是美国空军一种绝密的网络信息战武器，主要利用网络病毒入侵敌方通信系统、雷达站和计算机，尤其是与地面防空有关的系统。与主动强电磁干扰手段不同，依靠舒特系统，美军无须用导弹摧毁对方的通信系统和雷达，便能“凭空”渗透目标网络，使其呈现“麻痹”或“假死”状态，使己方的攻击机群能轻松完成预定的轰炸任务。凭借着舒特机载网络攻击系统，成功突破先进防空武器系统的严密防护，对纵深内的目标实施毁灭性突击。

### 3.4.4 震网病毒武器

#### 1. 震网病毒令世界震惊

早在 2009 年 6 月，震网病毒首例样本被发现。2010 年 6 月，震网病毒开始在全球范围大肆传播。2010 年 7 月，伊朗境内的诸多工业企业遭遇了一种极为特殊的计算机病毒袭



击,该病毒的主要攻击目标就是伊朗的布什尔核电站,直接导致了布什尔核电站推迟发电。截至2010年9月,已感染全球超过4.5万网络及相关主机。其中,近60%的感染发生在伊朗,其次为印度尼西亚和印度(约30%),美国与巴基斯坦等国家也有少量计算机被感染。2010年11月29日,伊朗总统内贾德公开承认,黑客发起的攻击造成伊朗境内一些浓缩铀设施的离心机发生故障。据报道,震网病毒可能破坏了伊朗核设施中的1000台离心机。由于震网病毒的侵袭,伊朗的核计划至少拖后了两年。信息安全界的许多专家将震网病毒攻击伊朗核设施列为2010年十大IT事件之一。

## 2. 概念与特点

震网病毒又名 Stuxnet 病毒,是第一个席卷全球产业界的专门定向攻击真实世界中基础(能源)设施的蠕虫病毒,比如核电站、水坝、国家电网、工业控制系统。它的复杂程度远远超出一般计算机黑客的能力。

震网病毒具有以下特点:

- (1) 与传统的计算机病毒相比,震网病毒不会通过窃取个人隐私信息牟利。
- (2) 由于它的打击对象是全球各地的重要目标,因此被一些专家定性为全球首个投入实战舞台的“网络武器”。
- (3) 一般通过移动载体进行传播,而无须借助网络连接。这种病毒可以破坏世界各国的化工、发电和电力传输企业所使用的核心生产控制计算机软件,并且代替工厂其他计算机“发号施令”。
- (4) 极具毒性和破坏力。震网病毒代码非常精密,主要有两个功能,一是使伊朗的离心机运行失控,二是掩盖发生故障的情况,“谎报军情”,以“正常运转”记录回传给管理部门,造成决策的误判。
- (5) 震网病毒定向明确,具有精确制导的“网络导弹”能力。它是专门针对工业控制系统编写的恶意病毒,能够利用 Windows 系统和西门子 SIMATIC WinCC 系统的多个漏洞进行攻击,打击的对象是 SIMATIC WinCC 的监控与数据采集(SCADA, Supervisory Control And Data Acquisition)系统,不再以刺探情报为己任,而是能根据指令,定向破坏伊朗核电站离心机等要害目标。
- (6) 震网病毒采取了多种先进技术。震网病毒从感染、传播,到实现对物理控制系统的攻击,综合利用了多个层次的漏洞攻击技术,涉及 Windows 等通用系统和工业控制系统等专用系统的开发利用技术,对病毒设计人员的技术能力要求很高。此外,为了防止多种防病毒软件的检测,该病毒还利用安全证书仿冒技术、Rootkit 技术等精心设计了一套自我保护机制。
- (7) 具有极强的隐身性。一般情况下,多数物理基础设施的工业控制系统都位于与互联网物理隔离的专用网络中。为此,震网病毒的设计者在确保其在互联网传播的同时,还专门设计了通过 U 盘进行传播的方式,感染物理隔离的专用网络。在“离线”操作的情况下,只要操作员将被病毒感染的 U 盘插入该系统通用串行总线架构(USB, Universal Serial Bus)接口,这种病毒就会在神不知鬼不觉的情况下(不会有任何其他操作要求或提示出现)取得该系统的控制权。

(8) 震网病毒结构非常复杂。震网病毒是迄今为止网络犯罪领域最为复杂的一款恶意软件。计算机安全专家在对软件进行反编译后发现，它不可能是黑客所为，而具备一定的高端性，其背后有强大的技术支撑和财政支持，应该是一个“受国家资助的高级团队研发的结晶”。美国《纽约时报》称，美国和以色列情报机构合作制造了震网病毒。

### 3. 发作过程

震网病毒的一般发作过程为释放文件、添加注册表键值、自身复制、释放.LNK 文件和创建互斥体，如图 3-10 所示。当感染了震网病毒的移动存储设备接入计算机后，病毒首先会释放文件，随后修改注册表信息，将自身复制到所有移动盘符目录下，接着释放.LNK 文件并隐藏相应文件和进程，达到消除修改痕迹的效果，最后释放其他组件文件，创建互斥体，禁止多个线程同时进入受保护的代码。

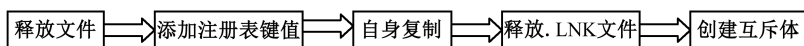


图 3-10 震网病毒的发作过程

### 4. 基本原理

震网病毒是自包含的程序，它能传播它自身功能的拷贝或它的某些部分到其他计算机系统中。与一般病毒不同，震网蠕虫不需要将其自身附着到宿主程序。

震网病毒的一般传播过程为漏洞扫描、攻击、传染、复制，如图 3-11 所示。在漏洞扫描过程中，由蠕虫的漏洞扫描功能模块负责探测存在漏洞的主机，当程序向某个主机发送探测漏洞的信息并收到成功的反馈信息后，就得到一个可传播的对象；攻击时，攻击模块按漏洞攻击步骤自动攻击扫描到的对象，取得该主机的权限，获得一个 shell；最后当需要复制时，复制模块通过原主机和新主机的交互将蠕虫程序复制到新主机并启动。



图 3-11 震网病毒的传播过程

震网病毒主要利用 Windows 系统漏洞通过移动存储介质和局域网进行传播，攻击以西门子公司控制系统（SIMATIC WinCC / Step7）的 SCADA 系统。SCADA 系统是一种广泛用于能源、交通、水利、铁路交通、石油化工等领域的工业控制系统。SCADA 系统不仅能够实现生产过程控制与调度的自动化，而且具备现场数据采集、监视、参数调节与各类信息报警等多项功能。震网病毒激活后，将攻击 SCADA 系统，修改其可编程逻辑控制器（PLC，Programmable Logic Controller），劫持控制逻辑发送控制指令，造成工业控制系统控制混乱，最终造成业务系统异常、核心数据泄露、停产停工等重大事故，给企业造成难以估量的经济损失，甚至给国家安全带来严重威胁。

震网病毒不通过互联网也能够传播，只要目标计算机使用微软系统，震网病毒便会伪装 RealTek 与 JMicron 两大公司的数字签名，顺利绕过安全检测，自动找寻及攻击工业控

制系统软件，以控制设施冷却系统或涡轮机运作，甚至让设备失控自毁，而工作人员却毫不知情。

## 5. 运行环境

震网病毒在以下操作系统中可以激活运行：

- (1) Windows 2000、Windows Server 2000;
- (2) Windows XP、Windows Server 2003;
- (3) Windows Vista;
- (4) Windows 7、Windows Server 2008。

当它发现自己运行在非 Windows NT 操作系统中，即刻退出。

被攻击的软件系统包括SIMATIC WinCC 7.0、SIMATIC WinCC 6.2，但不排除其他版本存在这一问题的可能。

## 6. 传播方式

由于震网病毒的攻击目标 SIMATIC WinCC 软件主要用于工业控制系统的数据采集与监控，一般部署在专用的内部局域网中，并与外部互联网实行物理上的隔离。为了实现攻击，震网病毒首先通过互联网等感染外部主机；然后利用 Windows 系统漏洞感染 U 盘，传播到内部网络；在内部局域网中，通过快捷方式解析漏洞、远程过程调用协议（RPC，Remote Procedure Call Protocol）远程执行漏洞、打印机后台程序服务漏洞、内核模式驱动程序漏洞、任务计划程序漏洞等多项系统漏洞，实现联网主机之间的传播；最后抵达安装了 WinCC 软件的主机，实现对工业控制系统的攻击。震网病毒采用多种手段进行渗透和传播，传播方式如图 3-12 所示。

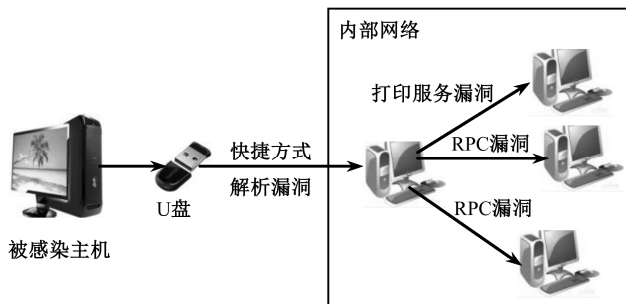


图 3-12 震网病毒的传播方式

### 3.4.5 数字大炮

数字大炮通过“路由自激”的攻击方式，利用互联网的结构漏洞来攻击其自身。从本

质上来说,数字大炮是一种新型的针对互联网路由系统的攻击方法,它将互联网路由系统作为目标,进行分布式拒绝服务攻击。数字大炮在攻击机理上没有重大突破,只是综合运用了多种已有的攻击技术,利用边界网关协议的特点,通过攻击互联网起关键作用的核心节点,达到瘫痪整个互联网的攻击效果。从应用层面来看,数字大炮所涉及的技术,还处于理论研究和仿真实验阶段,尚未在真实环境中得到具体应用,其威胁效果有待进一步研究和评估。

## 1. 互联网存在的结构漏洞

(1) 在网络上每分钟都有许多节点脱机,组成互联网的那些较小的网络,也就是人们所知的“自治系统”——能通过路由器互相通信。

(2) 当一个通信路线发生改变,附近的路由器会通过一个所谓的“边界网关协议(BGP, Border Gateway Protocol)”系统向其附近的路由器发出通知。这些路由器又接着向其他邻近路由器发出通知,最后将新路径的情况发布到整个互联网。

(3) 2007年2月发现的一种攻击方法叫作ZMW攻击(密歇根大学的3位华人研究者共同发现,并以各自姓氏首字母来命名),它通过扰乱BGP,使两个路由器之间的连接显示为脱机,从而切断这两个路由器之间的连接。美国明尼苏达大学马克斯·舒哈德教授及其同事将“ZMW攻击”方法扩展后形成的新型网络攻击方式,也称为“跨平面的会话终结”攻击,这使路由器数据层面上的攻击影响其控制层面,并将这种攻击造成的影响扩大到全球互联网,并模拟了其效果。

(4) 这种攻击需要一个巨大的“僵尸网络”——一个被木马感染的计算机组成的网络。马克斯·舒哈德估计25万台这样的计算机将足以摧毁互联网。僵尸网络经常被用来发动分布式拒绝服务(DDoS)攻击,这种攻击方式通过让网络服务器流量超载而使其死机。但是,马克斯·舒哈德这种新攻击方法却与此不同。

## 2. 数字大炮攻击的工作原理

与普通DDoS攻击不同,数字大炮的攻击对象是运行BGP的路由器。由于路由器作为网络层设备,一方面其应用服务种类较少,另一方面基于BGP的安全防御措施日趋完善;因此,要直接从路由器的控制平面对BGP本身实施攻击,难度是非常大的。而数字大炮攻击的工作原理不是通过获取路由器的控制权来实施攻击,而是利用BGP自身的特性,通过对路由器数据层面发起大规模DDoS攻击,使网络中路由器间互连链路反复拥塞,影响路由器控制层面的信息交互,造成BGP邻居的路由信息频繁抖动。具体工作原理如下:

(1) 攻击者要在僵尸网络中的计算机之间发送流量,建立它们之间的“路径地图”。然后他们要找到众多路径公用的一个连接,发动ZMW攻击摧毁它,使路由器间互连链路发生拥塞,途经这些路由器的转发路径将失效。附近的路由器会对此作出回应,发送BGP更新消息,沿途的每一跳路由器都要重新计算和生成自己的路由表;新的路由表生成后,将流量导向别的地方。在很短的时间之后这两个被切断的路由器会重新连接,并发送它们

自己的 BGP 更新信息，攻击流量由此会再次流入，让它们再次断开。

(2) 这一循环不断重复，每次断开和重建连接都会向互联网上的每一台路由器发送 BGP 更新消息。最后全世界每一台路由器都会接收到超出自身处理能力的更新消息。

(3) 在世界上每一台路由器都被占用的情况下，正常的路由中断无法得到修复，最终导致路由器的中央处理器（CPU，Central Processing Unit）、内存等资源被不断更新的路由计算耗尽，控制平面崩溃，从而使数据层面无法转发数据，互联网会变得千疮百孔，处于瘫痪状态，无法进行通信。马克斯·舒哈德认为这种情况需要数天时间才能恢复。

(4) 这种攻击一旦发动，就无法通过技术手段解决，只能由网络运营者互相口头交流。每个自治系统都必须关闭并重启，以清除那些 BGP 积压处理任务。

### 3. 数字大炮攻击的运作机制

要发动数字大炮方式的网络攻击，首先要确定攻击对象（目标），然后根据攻击目标建立攻击模型。

数字大炮网络攻击的对象不是具体的服务器或主机，而主要针对网络自治域之间运行外部边界网关协议（EBGP，External BGP）的互联路由器。网络运营商出于网络安全考虑，往往不会把核心链路的 IP 地址广播出去，因此，网络攻击方（黑客）必须设法找到拟攻击的网络链路的子网地址。在网络上，黑客可以通过所掌握的大量僵尸主机资源，使用 ICMP 协议进行大范围的端到端网络路径探测，如 Tracert（路由跟踪实用程序）测试，大致绘制出攻击对象的网络拓扑，并找到网络中数据传送核心的若干跳，所对应的链路就是网络核心路由器之间的互联链路，这些链路上的 EBGP 会话也就是数字大炮网络攻击的对象。经过马克斯·舒哈德及其同事在实验室的模拟实验预测，只要正确定位攻击对象（目标），采用足够流量大规模的数字大炮攻击，即可中断被攻击网络中 98% 的 BGP 会话。

### 4. 防止崩溃

(1) 过滤 ICMP。发起数字大炮的攻击者，为明确攻击目标，做好攻击的前期准备，首先会使用 ICMP 进行 Tracert 和 Ping 测试，来发现网络拓扑以及探测网络设备是否存活。如果在运营商网络中，所有关键的网络设备均采取过滤 ICMP 报文的措施，则可大大减少数字大炮网络攻击发生的可能性。

(2) 架设“影子网络”。在运营商网络间架设一张专用网络，专门用于传送控制平面的协议流量，把业务数据流和控制数据流用不同网络实现相互隔离；在网络攻击方控制“僵尸”网络实施数字大炮网络攻击时，攻击流量只能到达业务数据流所在的网络上，而无法到达专用网络，因而路由器之间的 BGP 会话连接不会受到攻击流量的影响。理论上，这种方法是可以完全抵御数字大炮网络攻击的，但是在实际网络部署中，等同于要为每个自治系统/自治域建立一张虚拟的影子网络，由于成本过高，可行性则较低。

(3) 保持 BGP 邻居长时间不中断。通过增大 BGP 邻居会话连接计时器数值，在 BGP 邻居互联链路发生拥塞，BGP 数据包无法正常交互时，可继续保持 BGP 邻居关系的建立状态，避免 BGP 会话连接中断，以此可以在一定程度上防范数字大炮网络攻击。但根

据研究者的模型，此方法必须让互联网至少 10% 的自治系统作出这种改变，并且要求网络运营者寻找其他方法监控连接的健康状况，要说服足够多的独立运营商作出这一改变将很困难。

(4) 利用服务质量 (QoS, Quality of Service) 机制保障控制层面所需资源。利用 QoS 机制，对通过路由器的不同数据流分配不同的转发优先级，把物理链路划分成多条逻辑通道，每个通道根据需要使用独立的队列算法进行排队，不同类型的流量彼此互不影响；通过给网络协议控制流量分配最高的优先级，避免协议控制流量和其他业务流量互相争用资源，以此来减弱和防范数字大炮网络攻击的影响。具体思路是：首先定义访问控制列表，以匹配特定控制层面的流量；再为控制层面流量预留相应的链路带宽（如确保链路带宽的 5%~10% 用于控制层面）；最后将 QoS 策略应用在互联端口的出方向。由于 QoS 策略只对端口出方向流量起作用，对入方向流量不起作用，因此需要互联双方运营商在互联端口上均部署对控制层面流量的带宽保障 QoS 策略，才能对双向流量起保障作用。

(5) 长效机制。要从根本上防范针对 BGP 协议的 DDoS 网络攻击，则必须对现有的路由器进行重新设计，包括设备硬件物理结构和控制平面的数据结构两方面，在硬件上确保路由协议控制平面和业务数据转发平面使用的资源相对独立，当业务数据平面出现问题时，不会扩散到控制平面。在极限情况下，即使链路因大量的网络攻击流量导致拥塞，控制协议数据流依然可以正常传送，BGP 邻居会话连接状态不会因为链路拥塞发生中断和抖动，这样才可以从根本上杜绝数字大炮网络攻击的威胁。

### 3.4.6 下一代干扰机

#### 1. 简介

下一代干扰机 (NGJ, Next Generation Jammer) 是美军未来电子战的支柱性武器，由美海军空战中心武器分部与雷声公司共同研发。与前一代电子战吊舱相比，NGJ 的最大特点是完全可编程，作战人员可根据目标特点，在数小时内设定关键的参数，对预定目标实施电子攻击。与前几代系统相比，下一代电子干扰机能成为一个开放式的结构、高功率与低功率、电子战/电子进攻系统家族的基础，具有可扩展的特点，其作战能力不再被硬件性能所固化，而更多地取决于软件的水平，从更深层次上说就是取决于软件编程人员的智慧，能从比今天更远的地方向敌人发动电子战攻击。而随着电子信息系统越来越广泛地应用于各类作战武器，以软件形式固化的人类智慧将成为武器技战能力提升的主要驱动力。

#### 2. 研究计划

在 NGJ 项目异常激烈的竞标中，雷声公司厚积薄发，最终于 2014 年 1 月赢得了价值 2.79 亿美元的研发合同，并在随后不到两年的时间里，顺利通过了两个重要的里程碑节点。

2014年10月完成了 NGJ 样机的首次飞行试验,2015年7月完成了 NGJ 全向等效辐射功率测试。2016年4月,美国海军宣布授予雷声公司总额达10亿美元的 NGJ 工程制造与开发合同。巨额的大单令行业振奋,也令竞争对手眼热……

NGJ 项目旨在取代老化的电子战发射机——特别是 AN/ALQ—99 电子战套件,这种干扰机是一种新型、可扩展设计的干扰机,能够用于应对不断升级的威胁。新型干扰机将主要用在 EA—18G “咆哮者”(Growler)电子攻击机上,这是波音 F/A—18 “超级大黄蜂”(Super Hornet)的一种改进版本,以满足机载电子战需求。

### 3. 原型舱试飞情况

2014年10月,雷神公司研制的下一代电子干扰吊舱的原型舱试飞。此次试飞主要为了判断干扰机对模拟敌方雷达威胁的干扰和破坏效果。原型舱是一个集成电子吊舱,包含集成在一个可自供电的吊舱前端的全数字化接收机、干扰发射器和有源相控阵雷达。这些武器都已经在实验室里进行了测试。原型舱被装在一架“湾流”公务机机身之下。飞机从美国加利福尼亚州波因特穆古海航站起飞,前往“中国湖”海军空战试验场进行测试。雷神公司在其公告中指出,这次试飞中,干扰技术、波束敏捷、阵列发射功率和干扰管理的结合有效应对了威胁系统,均达到或超过了测试目标。目前该项目已经步入正轨,进展顺利,几乎所有的关键技术都已成熟。

### 4. 采用的新技术

NGJ 上采用的新技术主要包括:

(1) 数字波束形成技术。NGJ 上应用了宽带电子操控天线阵列技术的最新成果。通过控制有源电子扫描阵列(AESA, Active Electronically Scanned Array)来产生敏捷、稳定和集中的干扰能量波束,提升了干扰的敏捷性和精确性。新的 AESA 天线经过合理排布,克服了电子扫描阵列的固有缺点(发射/接收机孔径不能覆盖大于180度的区域),可产生连续、扇形重叠、360度波束覆盖区域。

(2) 氮化镓发射组件。这种发射组件可以提升 AESA 的干扰功率和效率。用氮化镓电子元器件取代老旧的砷化镓技术,将有助于在不影响其性能的前提下显著减少重量和功耗,并明显降低成本。

(3) 采用波束敏捷干扰技术,增强抗干扰能力。该技术使得干扰机能够实现自动目标干扰,对目标威胁的程度进行优先级排序。其态势感知能力更强,干扰效果更好。

(4) 采用全数字化接收机。其集成先进的通信技术、计算机技术和大规模数字集成电路技术,增强信号情报搜集能力和干扰敌方防空系统的能力。尤其在复杂的敌对环境,数字化接收机将具有先进的探测、处理、区分并显示无线电频率信号的能力。

(5) 采用开放式和可重新编程的体系结构,并采用模块化设计。开放式体系结构使用现有技术生产具有开放式设计经验和标准的模块化、交互式系统,使得该系统便于改进和升级,利于控制成本。同时使得传统系统转变成一体化的任务包,促进 NGJ 在多平台间公用。

(6) 新的供电方式，依靠自身携带的冲压式空气涡轮（RAT，Ram Air Turbine）发电机驱动设备来进行工作。RAT 的好处是对接口要求不高，通用性强，拆装方便，容易做到各机型通用，尽量减少对载机的限制，大大扩展了各种吊舱的使用范围。

## 5. NGJ 具备的新能力

与 ALQ—99 相比，NGJ 不仅增强了传统电子吊舱的电子对抗能力，还因新技术的引入而具备了新的功能。它的新能力主要包括以下方面。

(1) 电子对抗和信号情报等功能。NGJ 将提供全频谱干扰能力，能让简易爆炸装置的遥控引爆失效，同时可以探测并干扰多种雷达和通信信号。基于情报设计理念的下一代干扰机将采用多个频段的子发射机，频段间交叠使用，更能满足作战使用要求。从发现到分析，再到对抗敌方先进雷达和通信系统，需要 NGJ 发挥更强的信号情报搜集和电子对抗能力。

(2) 网络作战能力：NGJ 能在指挥网络中植入病毒。NGJ 通过 AESA 辐射源生成远程数据流，这些数据波束含有专门的波形和算法，可以像钥匙那样去打开网络。由空中发动的网络攻击可以关闭工业系统以及核设施。这就可以间接解释美国空军一直在伊朗周边秘密使用 RQ—170 无人机的原因，而 NGJ 更会显著拓展这一能力。

(3) 智能干扰能力：准确地识别信号并确定其位置是干扰工作的关键。一旦锁定一个威胁，NGJ 将能够接收其发出的各种信号，在频率和波形等方面对于反干扰的各种变化做出反应，无须依赖于 EA—18G 飞机自身的电子支援措施来控制。

(4) NGJ 的最大特点是完全可编程，NGJ 将利用美国政府科研机构、高校和工业界的技术成果。例如，它将采用高速数-模转换等软件驱动型数字式技术，可实现迅捷的重新编程。作战人员可根据目标特点，在数小时内设定关键的参数，对预定目标实施电子攻击。与前几代系统相比，其作战能力不再被硬件性能所固化，而更多地取决于软件的水平，从更深层次上说就是取决于软件编程人员的智慧。而随着电子信息系统越来越广泛地应用于各类作战武器，以软件形式固化的人类智慧将成为武器技战能力提升的主要驱动力。下一代干扰机将成为一系列电子战和电子攻击系统的基础，基于开放式结构的系统架构，在软件驱动下，实现更加灵活的远距离电子攻击。

(5) 高可靠灵敏波束射频系统，一种软件可编程的无线电模拟装置，用软件控制多种功能，能把网络战功能、自我保护功能、雷达的电子攻击功能和其他功能结合在一起，其设计是灵活的，可变化的。因此，当威胁变化时，NGJ 的系统也可以随之发生变化，但射频系统依然可以提供可控的功率输出，完成相应的系统功能。

## 6. 边改进边部署

美国海军计划以“增量式”来部署 NGJ。在第一阶段（增量 1），投产和装备的 NGJ 主要针对中波段电子对抗能力，将在 2021 年部署，以使该干扰机实现初始作战能力。第二阶段（增量 2）针对低波段进行改进，初步计划在 2022 年部署。第三阶段（增量 3）的改进针对高波段电子对抗，初步计划在 2024 年部署。



通过互用性和扩展波段覆盖, NGJ 将提供对付更大范围内各种射频发射机的能力。目前, NGJ 的部署平台均确定为 EA—18G 电子战飞机, 该机典型的配置将是在机翼下携带 2 个“增量 1”干扰吊舱, 在机腹中线携带 1 个“增量 2”干扰吊舱。美海军的官员们表示, 未来还将把 NGJ 部署或集成到其他的有人机和无人机上, 如目前正在研发的“舰载监视与打击无人机系统”。此外, 海军陆战队的 F—35B 预计会是另一种载机平台。未来美军的计划是建立一支分布式空中电子攻击队伍, 其电子战能力将远远超越现有的任何系统。当给 EA—18G 和其他飞机配备上新一代电子干扰机时, 美军将会拥有一件具备更多功能的不只是发射导弹和炸弹的武器了——凡是现阶段在电磁频谱范围内工作的任何设备几乎都是 NGJ 可以干扰和攻击的目标。

### 3.4.7 高功率微波武器

#### 1. 高功率微波武器的发展

20 世纪 70 年代以来, 美、英、法、德、日和苏联等军事大国竞相开展了高功率微波源和高功率武器杀伤机理的研究。进入 80 年代, 由于高功率微波源理论取得了突破性的进展, 主要由微波源和效应牵引, 它们从实验室阶段转向实用化阶段。90 年代是应用牵引的高功率微波研究项目, 21 世纪才逐渐向军用平台和进攻型武器的方向过渡。高功率微波弹头已被美军用于实战, 数枚高功率微波炸弹配合其他武器曾使巴格达指挥系统一度中断。目前, 各军事大国已把高功率微波武器研制纳入其国防战略发展计划中。

#### 2. 基本概念

高功率微波 (HPM, High Power Microwave) 武器是把微波器件产生的微波能量聚在很窄的波束内, 经过高增益天线定向辐射出去, 以极高的强度照射目标, 产生杀伤和破坏效果的武器。HPM 武器的电磁波峰值功率在 100MW 以上, 频率在 1~300GHz 之间。

国外研制的 HPM 武器主要有投掷式单脉冲高功率微波弹和可重复使用的 HPM 武器两种类型, 它们又称为射频武器。微波弹实际上是一种以核爆炸或普通炸药爆炸为能源, 能一次性使用的 HPM 的小型装置 (或称电磁脉冲发生器), 一般由能源、HPM 发生器、大型聚焦天线、跟踪瞄准设备和其他系统控制等配套设备构成。HPM 弹头结构框图如图 3-13 所示。较小的微波弹由制导炸弹或巡航导弹来进行投掷, 当飞到目标附近时, 爆炸产生的脉冲可以使计算机和通信设备中的电路失效, 或擦除计算机内存。其作用距离在 400 米内, 在天气好时该系统的有效范围有足球场大小, 天气不好时范围会大大缩小。通过在导弹或炸弹战斗部上加装电磁脉冲发生器和辐射天线的方式构成, 利用炸药爆炸压缩磁通量的方法产生高功率的电磁脉冲。较大的可制成炸弹形式, 使用武器有导航攻击系统、能够投放全球定位系统 (GPS, Global Positioning System) 制导武器的战术飞机投放, 其能

源已从使用电源发展到使用核爆炸或常规炸药爆炸产生的能源，这是一项重大进展。

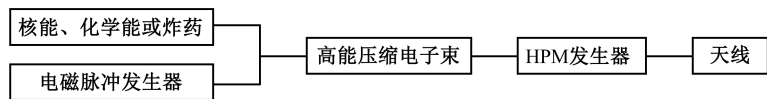


图 3-13 HPM 弹头结构框图

可重复使用的 HPM 武器，是多脉冲重复发射装置，它主要由电源 HPM 产生系统，目标捕获、跟踪、瞄准装置和发射天线等部分组成。多脉冲重复发射装置原理图如图 3-14 所示。发射天线将微波汇聚成方向性极强、能量极高的波束，在空中以光速直线传播，用于杀伤人员和电子设备。目前，美军把这种武器称为“超级干扰机”，可重复使用的 HPM 武器一般装在水面舰艇和地面车辆上。

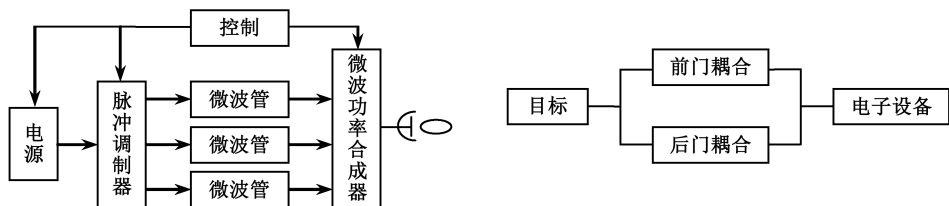


图 3-14 多脉冲重复发射装置原理图

HPM 武器是未来电子战中对付电子设备和武器系统的新一代电子战武器，是电子战武器系统及其技术一次新的革命。它不仅可以与雷达兼容构成一体化系统，实施低功率探测、跟踪目标，对目标进行干扰，还可以迅速提高功率，对目标实施硬杀伤摧毁，或者对目标的电子设备实施破坏，或者对人员进行杀伤使之丧失战斗能力。

### 3. HPM 武器的特点

与各类已有的传统武器相比，HPM 具有以下优点：

(1) 能够全天候作战。HPM 武器靠发射到空中的强电磁波对目标进行破坏和杀伤，而这种电磁波在大气中不存在严重的传输问题，因此 HPM 武器全天候运用能力极强，可与高能激光武器进行优势互补。

(2) 具有很强的针对性。由于微波射束能量集中，一般只对目标本身的某一部位或目标内的电子设备造成破坏。避免了大规模地杀伤平民和破坏环境。HPM 武器并非摧毁整个目标，而是通过破坏对方作战平台，使其作战平台失去控制和作战能力，从而达到“不战而屈人之兵”的效果。

(3) 对瞄准精度要求不高。凭借微波发射的射频波波束比较宽，可以照射到整个目标这一特点，HPM 武器在目标的瞄准和跟踪方面与常规武器相比精度要求较低，然而其击中概率却比任何常规武器高出约一个数量级。这使得利用 HPM 武器来对付敌方隐身军事目标成为可能。

(4) 可进行探测与跟踪打击。HPM 武器类似于雷达系统，可对目标进行探测和追踪，

继而利用 HPM 杀伤目标，由于电磁波在大气和真空中以近乎光速传播，故在各种不同的大气条件下可达到一发击中的效果。

(5) 用电源代替弹药。由于 HPM 武器依靠电源进行工作，其唯一的消耗就成为常规发电机和交流发电机所需要的燃料，在作战行动中无须供应弹药，从而减轻了后勤保障工作的压力。

(6) 是“万能”的“全才”。HPM 武器是一种打击目标全面、能够全天候使用、能多平台搭载、能够作战与维和行动混用的真正的“多能”武器。

(7) 有高效的能力。HPM 武器是一种效率极高的武器。首先，微波武器是一种“斩首”“掏心”的武器。它常常被用作摧毁敌方的指挥自动化系统这个军队的“首脑”，破坏各种武器的“心脏”——电子控制设备，使敌方无首无心，自然也就无力作战。其次，微波武器是一种一劳永逸的武器。微波武器是靠熔化、烧毁敌方电子设备中的半导体元器件，形成对电子设备的永久性破坏，使电子设备无法再恢复功能。

(8) 隐蔽性好。工程技术中的某些瓶颈问题一旦解决，微波源可做到很小，从而达到秘密攻击目标，给敌方以突然打击，继而造成巨大心理压力的效果，这也正符合心理战的要求。

(9) 是全方位战场的延伸者。把它装载在无人机上后，人们就能够利用隐性技术深入敌方重兵把守的腹地，可用各种方式使敌军的精密通信设备和电子设施瘫痪，而且可以深入敌军防卫严密的地区，摧毁对方的防空雷达、通信设备、指挥所和控制中心的电脑、生化武器仓库或生产基地，从而使战争延伸到敌人的大后方。

#### 4. 系统组成

HPM 武器的组成框图如图 3-15 所示，初级能源（电能或化学能）经过能量转换器（强流加速器或爆炸磁压缩换能器等）转换为高功率强流脉冲相对论电子束（高功率脉冲功率源）。在特殊设计的 HPM 器件内，经过强电子束发生器，与电磁场相互作用，将能量交给电磁场，产生高功率的电磁波，即微波源。这种电磁波经低衰减的定向发射装置（如定向辐射天线）变成高功率微波束发射到目标表面后，经过目标的天线或传感器等（称为前通道）或经过散热小孔或缝隙等（称为后通道）耦合进入到目标的内部，干扰电子传感器或烧坏电子元器件（如保险丝、晶体管、集成电路等），使其控制电路失效而不能作战，或对于具有引信装置的导弹、大口径火炮等目标也可毁坏其结构，使其过早自爆。



图 3-15 HPM 武器的组成框图

#### 5. 原理

HPM 武器除一般武器必备的捕捉、跟踪、瞄准目标等辅助系统外，还应由初始能源、激励电源、高功率微波源和发射天线等组成，并由跟踪瞄准引导设备进行定向，由作战平台运载。HPM 组成示意如图 3-16 所示。

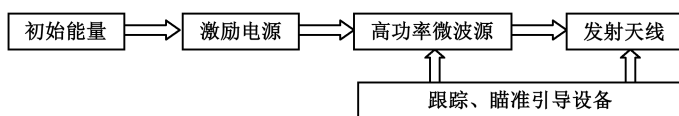


图 3-16 HPM 组成示意

初始能源可以是电容器组储存的电、燃油或者燃煤、武器炸药中储存的化学能，其作用是激励电源提供能源；激励电源则采用强流电子束发生器，为强流电子束发生器提供电能的供电设备，或者初始能源为电能的能量转换设备。发射天线与控制系统的作用是将高功率微波会聚成针状波束，射向目标。此外，目前高功率微波源可以选用相对论速调管、多波切伦科夫振荡器、高功率回旋管、相对论磁控管、虚阴极振荡器、波束管离子产生器及自由电子激光器等。它与常规微波源的主要差别是采用强流相对论技术，即在兆伏级激励电压和数十千安量级激励电流的作用下，从阴极发射出能量极高的电子射束；当这些电子射束进入器件内相互作用区时，其运动动能转换成微波场的电磁能，继而加速产生高功率微脉冲射束。

## 6. HPM 毁伤机理分析

高功率微波脉冲对系统及元器件的破坏机制主要有以下几种：

- (1) 高压击穿。电磁能接收后转化成高电压或大电流，由此引起节点、部件或回路间击穿。
- (2) 器件烧毁。包括半导体器件的结烧蚀、连线熔断等。
- (3) 微波加温。微波可使金属、含水介质加温，使器件不能正常工作。
- (4) 电涌冲击。脉冲高电压、大电流进入系统、设备，电路像电涌一样烧毁器件、电路。
- (5) 瞬间干扰。当进入的功率较低，导致电路出现干扰，不能正常工作。

HPM 武器几乎对所有利用电子设备工作的系统都有效。前门耦合和后门耦合是高功率微波能量进入电子系统的两种途径，前门耦合是通过发射或接收系统的天线进入形成的耦合；后门耦合则是通过一些缝隙、引线、电缆、窗口，甚至纤维玻璃、环氧树脂等进入形成的耦合。使用了天线的电子系统，如情报探测系统、侦察监视系统、通信系统、导航系统、直升机引导系统等构成了  $C^4ISR$  的主要框架，当受到高功率微波照射时，这些系统在天线的工作频率上前门耦合最强。感应信号的大小与进入壳体内的微波能量的大小和谐振性能的好坏有关，对小尺寸外壳连线耦合的测量显示：在不同频率上有很强的谐振效应，在与外壳开口大小接近的外壳谐振频率上耦合最强，缝隙中的耦合电场约增强至入射微波电场的 8 倍；高于或低于外壳谐振频率时，耦合都有所下降。

高功率微波对电子系统的损伤程度与进入电子系统的能量和电子系统本身的易损性有关，在 HPM 武器发射的有效功率确定的情况下，到达目标的能量  $P_1$  与微波武器距目标的距离  $R$ 、目标的有效雷达反射面积  $\sigma$  有关：

$$P_1 = \frac{P_a G_a}{4\pi R^2} \quad (1)$$

式中： $P_a$  是 HPM 武器的发射机功率； $G_a$  是 HPM 武器的发射机天线增益。

当到达目标的微波功率密度达到  $0.1 \sim 10 \text{ kW/m}^2$  时，可使电子设备的微波元器件性能降低或失效，例如：使小型计算机的芯片失效或烧毁；使探测系统、C<sup>4</sup>ISR 和武器系统中电子元件失效和烧毁。当到达目标的微波功率密度达到  $0.1 \sim 1 \text{ MW/m}^2$  时，高频微波辐射形成瞬变电磁场，可使金属表面产生感应电流，并通过天线、导线、电缆和各种开口或缝隙耦合到卫星、导弹、飞机、舰艇、坦克、装甲车辆等内部电路产生感应电压，破坏各种敏感元件，如传感器和电子器件，使元器件产生状态反转、功能紊乱、击穿、出现误码、记忆信息抹掉甚至永久失效等。当到达目标的微波功率密度达到  $10 \sim 100 \text{ MW/m}^2$  时，会使目标在很短的时间内遭受高压而破坏，甚至能够提前引爆导弹中的战斗部或炸药。

## 7. 关键技术

HPM 武器系统的研制涉及几项关键技术，具体包括脉冲功率源技术、高功率脉冲开关技术、能量转换技术、高功率微波源技术、定向辐射天线技术、超宽带和超短脉冲开关技术等。

(1) 脉冲功率源技术。脉冲功率技术的任务是对大量能量进行调节，在时间上将其压缩到更高的功率，以便提供极高峰值功率和低占空系数的脉冲功率能流。目前，通常的脉冲功率源有 Marx 发生器、Tesla 变压器、磁流体发电机、磁通压缩发生器等。脉冲功率源技术的关键部件是能量储存装置，例如，静电能储存在电容器内，磁能储存在电感器内，动能储存在转动飞轮内，化学能储存在诸如爆磁压缩发生器中。能量储存装置向脉冲形成网络放电（多级能量存储与转换），并将能量压缩成短脉冲，从而大大提高功率，并将其耦合负载。

(2) 高功率脉冲开关技术。一般情况下，脉冲功率源产生的脉冲不能直接有效地激励高功率微波源，因为脉冲的各项参数并不适合高功率微波源的正常运行，因此需要脉冲开关将其脉冲峰值、上升前沿和脉宽变得更为理想，使其能够有效地激励微波源器件。

(3) 能量转换技术。目前，将脉冲功率技术形成的高功率电能脉冲转换成电子和离子的动能，是由“强流脉冲型加速器”等完成的。这种加速器技术通常分为射频加速器、感应加速器和强流脉冲加速器 3 类。俄罗斯科学家们使用一种能够装在武器中的“课桌大小”的爆磁压缩发生器，能把爆炸能量转换成强大的电磁脉冲。试验表明，这种爆炸磁通压缩发生器能为“单发射”微波提供能量达到  $100 \text{ MJ}$ （兆焦耳）。

(4) 高功率微波源技术。高功率微波源是微波武器的核心组件，而作为武器用的高功率微波源，要求它产生的微波功率比现今雷达用的微波源功率要高几个量级。平常所说的微波由于输出功率太低，因而只能用作探测、侦察、通信等使用，而不能用作杀伤摧毁性武器。20 世纪 70 年代以来，脉冲功率技术有了重大突破，电子能量（或脉冲高电压）为数百万电子伏、电子束流强度为数百万安培、峰值功率达到千亿瓦以上的强流电子束加速已在实验室建成并运转，利用这种电子束流激励功率从千兆瓦到数万兆瓦的微波脉冲，现

已变成现实。目前高功率微波源发展迅速，主要有自由电子激光器、返波振荡器、回旋管振荡器、相对论磁控管振荡器、虚阴极振荡器、轴向激励的虚阴极振荡器、多波切伦科夫发生器、等离子体辅助慢波振荡器、单脉冲返波振荡器、场致辐射振荡器等。

(5) 定向辐射天线技术。定向辐射天线是高功率微波源和自由空间的界面。与常规天线技术不同，高功率微波定向能武器用的天线，具有两个基本的特征：一是高功率；二是短脉冲。为满足定向能武器的需要，天线应满足以下要求：很强的方向性，很大的功率容量，带宽较宽，重量、尺寸能满足机动性要求并具有适当的旁瓣电平和波束快速扫描的能力。这种天线包括一个高功率微波源，其释放的能量经真空波导传输到后面的波束成形网络（例如波导的移相、合成或分相等），然后进入一馈电阵列。

(6) 超宽带和超短脉冲技术。超宽带技术是一种新型的无线通信技术。它通过对具有很陡上升和下降时间的冲击脉冲进行直接调制。脉冲宽度约十几皮秒或几纳秒，占空比为1%甚至更小；频率范围可以从0一直延伸到几十兆赫兹；无载波，无频谱搬移，属基带通信。超宽带技术具有对信道衰落不敏感、发射信号功率谱密度低、低截获能力、系统复杂度低、数据传输率高、系统容量大，对多径具有鲁棒性、保密性和安全性好、结构简单、成本低，能提供数厘米的定位精度等优点。超短脉冲是延续时间在飞秒（ $10^{-15}$ 秒）数量级或更短的电磁脉冲。这样的脉冲时间宽度非常短、瞬态成像、超快开关，适合于高速通信。

## 8. 作战运用形式

HPM 武器作战运用主要有两种形式：一种是地基固定式，以保护首脑机关的指挥中心、导弹发射阵地、重要城市、工厂、仓库、基地，配置若干个 HPM 武器系统，攻击来袭飞机、导弹，扰乱或摧毁这些来袭目标所使用的指挥、搜索、控制系统，使其丧失战斗力；另一种是机动式，可分为机载、舰载、车载和弹载等几种方式，前三种分别以飞机、舰艇、车辆为平台，攻击空中、海上、陆地的各种目标，弹载则以各种导弹、炸弹为载体，利用爆炸能量产生微波攻击各类目标。随着航天技术的快速发展，微波武器的第三种作战形式已走进人们的视线，即将微波武器以航天器为平台，攻击卫星等太空目标或地面、海上乃至空中目标。显然，第三种作战方式将随着太空战场越来越被重视而看好。

## 9. 攻击敌方信息链路或节点的主要手段

HPM 武器主要用于毁伤电子设备，使其功能降级，甚至完全不能工作，来瓦解敌方武器的作战能力。其主要作战对象包括雷达、预警飞机、通信电子设备、军用计算机、战术导弹与隐身飞机等。在相对目标适当的距离上，HPM 武器发射的电磁脉冲能够毁伤敌军电子侦察与监视系统、军事网络电子信息系统、综合电子信息系统信息传输链路设备、卫星通信地面站或舰船站、卫星导航定位接收机等，降低敌军获取、分发综合电子信息系统信息，以及卫星导航定位的能力；可以瘫痪敌国重要政治、经济中心的计算机网络，毁伤卫星广播电视信号转发节点和无线通信网络节点，使其通信网络服务能力降级甚至失效；利用机载微波武器发射的微波波束辐照来袭导弹，可使导弹偏离目标或提前引爆，从而对高价值飞机起到自卫防护作用。在科索沃战争中，微波脉冲弹的使用，使南联盟部分

地区各种通信设施瘫痪了3个多小时。美军的AGM—86C巡航导弹弹头武器装配高功率微波器后,一旦在战场上使用,将使目标附近大范围区域内的电子设备失灵,产生的破坏力比相同大小的常规弹头高许多倍。从发展的趋势看,HPM武器也将是未来战时摧毁敌国家、国防信息基础设施的主要手段。这种武器投入使用后,不仅可能给21世纪的武器系统带来新变化,而且还有可能利用这种武器及其对抗手段来控制21世纪的战场,并对未来战争的作战方式带来重要影响,成为核威慑条件下信息化战争的另一种撒手锏。

## 10. 发展方向

HPM武器从实验室装置转向实用化武器,并逐渐向军用平台和进攻型武器方向过渡,HPM武器技术也正向小型化、高效率、模块化方向发展。目前,各军事大国已把HPM武器研制纳入其国防战略发展规划中。美军在HPM的研究方面投资最多,每年仅花费在脉冲源上的投资就达数亿美元。2012年,美国空军将HPM武器装在无人作战飞机上,用来对付防空导弹、雷达、车辆,烧坏武器关键装置的电子部件。《美国空军2025年战略规划》在未来武器构想中提出发展空基HPM武器,要求这种武器对地面、空中和空间目标具有不同的杀伤力,用一组低轨道卫星把超宽带微波投射到地面、空中和空间目标上,在几十到几百米的范围内产生高频电磁脉冲,摧毁或干扰目标区内的电子设备。美军现有技术较为成熟的HPM武器主要有微波弹、非致命性定向能武器、电磁脉冲炸弹等。美军近年来一边发展高功率微波技术,一边研制武器样机,并在试验场演示验证,甚至在战场中使用。在高功率微波产生源、高功率微波发射与传输技术、高功率微波效应和防护技术等方面的研究处于领先;在高功率微波弹头小型化、波束精确控制方面取得重大突破。俄罗斯是研究发展HPM武器技术最早的国家之一,在重复频率脉冲功率源技术和高功率微波产生技术方面处于国际领先地位。俄罗斯早在十多年前就拥有微波弹,在几年前就为SS—18洲际导弹装备了电磁脉冲弹药。我国高功率微波技术获得了阶段性突破,在高功率微波源技术、高功率微波发射与传输技术、高功率微波效应技术等方面的关键技术指标达到国际先进水平。未来,HPM武器一旦投入作战使用,战场可能会在很大程度上进入以微波和光子代替导弹的新时代。

## 11. 防护措施

对于网络空间系统而言,应结合结构特性并综合考虑其作战效能,有目的、分重点地实施防御,加强对高功率微波的防护措施。

- (1) 尽量减少暴露部分,减少接收的电磁波能量,接收天线的设计应具有良好的频段及滤波特性,尽量抑制无用的电磁波,并采用滤波接插头。
- (2) 采用良好的屏蔽措施,有效地堵塞孔洞及缝隙,以防止高功率微波的进入。
- (3) 在系统的出入口处采用电涌保护器件,防止电涌电流的进入。
- (4) 广泛采用微波吸收材料作为充填材料及连接垫片等吸收微波能量。
- (5) 在设备设计阶段,要重点考虑电磁兼容特性,并在安装过程中保证符合电磁兼容标准。

(6) 采用时间回避法，即利用灵敏度极高的传感器在高强度电磁场到来之前关机，将电源切断，或迅速将信号转移至非发挥作用的储存器中，等电磁干扰过后再恢复工作。

## 3.5 网络空间防御武器

网络空间防御武器主要包括攻击检测、网络安全监控与告警、网络防火墙、数据加密、网络安全协议、病毒免疫卡、病毒检测与消除、审计跟踪、安全密钥管理等，其中加密设备和防火墙始终是网络防护的两大核心武器。具有代表性的是美国空军“网络诱骗”系统、“网络狼”软件系统、深查威胁管理系统、深查告警服务系统、网络漏洞扫描仪；美国陆军入侵检测系统和美国空军抗太阳辐射型空间路由器；美军的“网络盾牌”，特别是美军的深查威胁管理系统，它可以对网络信息系统所面临的潜在威胁做出告警并推荐相应的反应手段。下面对一些常用的和比较典型的网络空间防御武器加以介绍。

### 3.5.1 网络空间常用的防御武器

网络空间常用的防御武器主要有防病毒工具、防火墙、数据加密系统、安全操作系统、入侵检测系统（已在第 3.3.6 节进行了介绍）、备份与恢复系统等。

#### 1. 防病毒工具

防病毒工具能够检测和清除病毒，包括各种防病毒软件或防病毒卡（硬件）。目前比较著名的防病毒软件主要有卡巴斯基、诺顿、大蜘蛛、熊猫卫士、赛门铁克、小红伞、McAfee、avast、360、电脑管家、金山毒霸、瑞星、江民和趋势等。防病毒卡是病毒防护的硬件产品，将病毒防护程序固化，就成为防病毒卡，如使用较多的“瑞星卡”“求真卡”等。

按工作原理，防病毒工具可分为扫描程序、完整性检查程序、行为封锁程序、启发式分析程序，以及访问控制程序。

(1) 扫描程序。其优点是检测速度快、误报少，通常都能够恢复被病毒感染的文件和数据。但在使用中的不便之处就是需要经常升级，而且如果没有适当的扫描引擎，就很难对付变形病毒。目前世界最先进的病毒扫描引擎为所罗门博士（Dr Solomon）公司所拥有，能够有效地对付可变形病毒。在 Dr Solomon 被美国网络联盟公司（NAI, Network Associates Inc）收购之后，这种优秀的病毒扫描引擎已纳入了 NAI 的 VirusScan 防病毒软件之中。

(2) 完整性检查程序。它能够检查可执行程序是否已被替换或更改。完整性检查程序的优点是程序本身无须升级，但其缺点是无法检测病毒，而只是发现程序的变化，无论这种变化是不是由于病毒所引起的，所以其误报率较高。要想弥补完整性检查程序的这些缺



点,就必须将其与扫描程序结合在一起使用。

(3) 行为封锁程序。其工作原理基于以下规律:正常合法的程序都会遵从一系列的规则,而病毒也有其一系列的规则。但由于程序的多样性和富于变化,封锁程序按固定规则检查的手段也经常会出现误报,且概率较高。

(4) 启发式分析程序。它能够扫描可执行代码或相关技术,一旦发现可疑部分即向用户发出警告。这种方式的误报率极高。

(5) 访问控制程序。它能够阻止未获授权的程序在计算机上进行安装,同时也能够阻止对磁盘的未授权访问和使用,以此来阻止病毒进入计算机。这种手段的优点是能够限制病毒的进入,并且本身无须升级服务。但此种手段不能识别病毒,必须与其他识别手段一同使用才能够达到清除病毒的目的。对于通过电子邮件和互联网传播的病毒则无能为力,同时它也部分地限制了系统的可用性和灵活性。

综上所述,我们不难看出目前仍然是扫描程序在技术上占据优势。它能够正确识别已知病毒,其误报率远远低于其他手段,并能够完成清除和恢复工作。所以用户在选择防病毒软件的时候,其主体应该为扫描程序,而其他的手段只能作为辅助工具。

## 2. 防火墙

防火墙是受保护的内部网和不被信任的外部网络之间和专用网与公共网之间的界面上构造的一道电子安全保护屏障,它通过在网络边界上建立相应的网络通信监控系统来隔离内部和外部网络,以阻挡来自外部网络非授权访问或非法入侵。它是一种计算机硬件和软件的结合,主要由服务访问政策、验证工具、包过滤和应用网关4个部分组成。防火墙是具体实施访问控制策略的系统,用来强化网络安全策略,加强网络间访问控制,对网络存取和访问进行监控审计,防止各种信息的泄露,阻止向外非法传递信息及破坏内部网络等。防火墙本身具有高可靠性,不受外部攻击影响。要有效保障安全,必须保证内外通信确实通过防火墙,只允许内部访问策略授权的通信通过。另外防火墙要具有易用性好,即使用界面友好,交互性强等特点。防火墙已经出现多年,大体可分为四代:包过滤防火墙、电路层防火墙、应用层防火墙(代理防火墙)、复合型防火墙。目前,防火墙技术发展迅速,最新的防火墙已经集成了很多网络边缘功能及网管功能,如虚拟专用网(VPN)功能、计费功能、流量统计与控制功能、监控功能、网络地址转换功能等。

## 3. 数据加密系统

数据加密系统是指采用加密技术,能对网络中传输和存储的数据提供加密和解密一体化功能的系统。目前数据加密实现方法主要有两种:软件加密和硬件加密。

软件加密就是用户在发送信息前,先调用信息安全模块对信息进行加密,然后发送,到达接收方后,由用户使用相应的解密软件进行解密并还原。采用软件加密方式有以下优点:已经存在标准的安全应用程序编程接口(API, Application Programming Interface)产品、开发时间短、研发成本低、部署维护方便、兼容性好。但是采用软加密方式,有一些安全隐患:第一,密钥的管理很复杂,这也是安全API的实现的一个难题,从目前的几个

API 产品来讲，密钥分配协议均有缺陷；第二，使用软件加密，因为是在用户的计算机内部进行，容易给攻击者采用分析程序进行跟踪、反编译等手段进行攻击；第三，软件加密速度相对较慢。

硬件加密系统可以描述成通过使用系统硬件资源安全地、便捷地对上层应用提供包括密码运算、密钥存储、随机数生成在内的诸多安全服务。硬件加密将加密芯片、专有电子钥匙、硬盘一一对应到一起时，加密芯片将把加密芯片信息、专有钥匙信息、硬盘信息进行对应并做加密运算，同时写入硬盘的主分区表。这时加密芯片、专有电子钥匙、硬盘就绑定在一起，缺少任何一个都将无法使用。外界只能通过定义好的接口调用其中功能，不能直接访问其中的敏感信息，也不能对其中进行的运算任务进行干预。任何对密码设备的非法访问都将被加密系统阻止。当非法访问严重威胁加密系统安全时，加密系统可以采取包括自毁在内诸多防护措施。硬件加密速度较快，一般来说，硬件加密所需的时间仅为软件加密时间的千分之一；可以采用标准的网络管理协议来进行管理，比如，简单网络管理协议（SNMP, Simple Network Management Protocol）和公共管理信息协议（CMIP, Common Management Information Protocol）等，也可以采用统一的自定义网络管理协议进行管理。因此密钥的管理比较方便，而且可以对加密设备进行物理加固，使得攻击者无法对其进行直接的攻击。市场上的硬件加密产品有独立式的保密机，也有卡式的，可插在计算机的扩展槽内。此外，也有其他形式，如智能卡等。保密机在军事领域较为常见，选择时应注意速度，是否便于使用，特别其密钥管理是否不需或很少需要用户干预等。

#### 4. 安全操作系统

安全操作系统是指计算机信息系统在自主访问控制、强制访问控制、标记、身份鉴别、客体重用、审计、数据完整性、隐蔽信道分析、可信路径、可信恢复等十个方面满足相应的安全技术要求的系统。

安全操作系统主要特征体现在四个方面：一是最小特权原则，即每个特权用户只拥有能进行自己工作的权力；二是自主访问控制和强制访问控制，包括保密性访问控制和完整性访问控制；三是安全审计；四是安全域隔离。只要有了这些最底层的安全功能，各种混为“应用软件”的病毒、木马程序、网络入侵和人为非法操作才能被真正抵制，因为它们违背了操作系统的安全规则，也就失去了运行的基础。

一个操作系统的安全性可以从以下四个方面考虑：

- （1）物理上分离。进程使用不同的物理实体。
- （2）时间上分离。具有不同安全要求的进程在不同的时间运行。
- （3）逻辑上分离。用户感觉到他的操作是在没有其他进程的情况下进行的，而操作系统限制程序的存取使得程序不能存取其允许范围外的实体。
- （4）密码上分离。进程以一种其他进程不了解的方式隐藏数据及计算。

操作系统安全的主要目标是：按系统安全策略对用户的操作进行存取控制，防止用户对计算机资源的非法存取；标识系统中的用户和身份鉴别；监督系统运行的安全性；保证系统自身的安全性和完整性。

操作系统的安全机制包括硬件安全机制和软件安全机制。硬件安全机制涉及存储保护、运行保护和 I/O 保护等内容。下面着重讲述软件安全机制。

软件安全机制主要包括以下几个方面：

(1) 用户标识与鉴别。标识与鉴别是涉及系统和用户的一个过程。标识是系统要标识用户的身份并为每个用户取一个名称——用户标识符。将用户标识符与用户联系的动作称为鉴别，为了识别用户的真实身份，它总是需要用户具有能够证明其身份的特殊信息。

(2) 存取控制。在计算机系统中安全机制的主要内容是存取控制。它包括以下 3 个任务：授权（确定可给予哪些主体存取客体的权利），确定存取权限，实施存取权限。在安全操作系统领域中，存取控制一般都涉及自主存取控制和强制存取控制两种形式。

(3) 最小特权管理。将超级用户的特权划分为一组细粒度的特权，分别给予不同的系统操作员/管理员，使各种系统操作员/管理员只具有完成其任务所需的特权，从而减少由于特权用户口令丢失或错误、恶意软件以及误操作所引起的损失。

(4) 可信通路。在计算机系统中，用户是通过不可信的中间应用层和操作系统相互作用的，操作系统必须保证用户在与安全核心通信时不会被特洛伊木马截获通信信息，提供一条可信通路。

(5) 隐蔽通道。隐蔽通道是允许进程以危害系统安全策略的方式传输信息的通信信道。系统设计时要进行隐蔽信道分析，采取一些措施在一定程度内清除或限制隐蔽通道。

(6) 安全审计。安全审计是对系统中有关安全的活动进行记录、检查及审核。主要目的就是检测和阻止非法用户对计算机系统的入侵，并显示合法用户的误操作。安全审计作为一种事后追查的手段保证系统的安全性。

(7) 病毒防护。一般来说，完全防止计算机病毒是非常困难的，但是通过安全操作系统的强制存取控制机制可以起到一定的保护作用。

## 5. 备份与恢复系统

网络备份与恢复系统能在网络系统硬件、软件或数据遭到敌方破坏时，及时地采用数据备份与恢复的方法进行恢复。主要包括网络硬件设备（如交换机、服务器和电源等）的备份与恢复、数据备份与恢复等。其中，数据备份是关键。

一般来说，系统由数据备份系统和数据恢复系统两部分构成。数据备份系统所使用的存储介质主要有磁带、磁盘和光盘等，有三种工作方式：完全备份、增量备份、差别备份。

服务器一旦崩溃或由于某种故障而完全停止运行，就必须使用恢复系统重建服务器的系统软件和数据。首先应安装服务器操作系统、所需的驱动程序、所需的服务软件包、修补程序，安装备份软件；然后恢复最后一次完全备份磁带，恢复需要的所有增量备份或差异备份磁带。

备份虽然是保护信息的良好方法，却不是服务器恢复的有效手段。恢复崩溃的服务器是一项耗费大量时间和精力的工作。另一种可选的方法是使用一种专门用于服务器恢复的

软件包。一般情况下，这些软件包都会生成一些保存有服务器镜像文件的启动盘。这些启动盘可以使服务器在没有系统的情况下启动，然后服务器恢复软件回访以前生成的镜像文件，并把所有的数据恢复到服务器上。服务器重新启动即可恢复运行。

目前，一些厂商已经提供了将服务器恢复功能和备份解决方案集成在一起的软件产品，如 Computer Associates 公司提供的 ArcServer 产品序列。如果用户每天网上使用 ArcServer 软件进行备份，它同时会生成一份 ArcServer 灾难恢复选项。由于 ArcServer 灾难恢复选项可以读取 ArcServer 的备份磁带，使得灾难恢复程序能够自动使用最后一次完全备份的磁带恢复服务器的配置。

应该指出的是，服务器灾难恢复解决方案将会把整个系统以镜像文件形式保存，不利于用户访问单独的文件，因此，在使用服务器灾难恢复解决方案的同时，必须保持常规的备份方案，以应付偶尔丢失文件时需要进行的恢复工作。

### 3.5.2 网络诱骗系统

目前，网络防御还主要依靠被动防御技术，虽然能在一定程度上保证网络的安全，但随着网络安全问题的日益严重，需要一种纵深的、动态的网络防御技术。在此背景下，网络诱骗技术的研究逐渐成为人们关注的热点，而且在众多领域发挥了关键性的作用。

#### 1. 基本概念

所谓网络诱骗技术就是在网络中伪造一些安全漏洞和有价值的资源，并使网络入侵者相信这些安全漏洞和资源是真实的。网络诱骗系统内部运行着各种特殊用途的记录程序，在系统被入侵后记录黑客的行为，通过跟踪、监视网络入侵者的踪迹来分析其进攻的意图和采用的工具与技术，从而有的放矢地加强自身网络的安全防御，进一步提高抵抗类似入侵事件的能力，以便掌握最新的安全技术。同时，利用网络诱骗技术也可以诱导网络入侵者一步一步地走入设置好的网络陷阱，增加入侵者的工作量和入侵复杂度，消耗入侵者的资源，从而保护真正有价值的网络资源。

网络诱骗系统是一个安全资源，它的价值就在于被发现、被探测、被攻击，并借此收集所需要的入侵证据。一个设计出色的网络诱骗系统要拥有以下功能：欺骗、发现攻击、产生警告、强大的日志记录能力，并在适当的时候能够协助调查。

#### 2. 网络诱骗系统的分类

根据不同的考虑，网络诱骗系统可以有多种分类方法，从结构组成上考虑，可将它们划分为两类：虚拟诱骗系统和真实诱骗系统。

虚拟诱骗系统大多用仿真软件来实现,因此黑客的入侵深度局限于这个仿真系统所模拟的程度。虚拟诱骗系统能够伪装成某个服务器进程,侦听外部连接并且与试图入侵它的黑客进行交互。在默认情况下,诱骗系统可以监测和记录一切 TCP 和 UDP 端口,也可将诱骗系统配置成检测某个具体的端口。例如,虚拟诱骗系统可以利用仿真软件伪装成一个 Telnet 服务进程,监视与 Telnet 相关的 23 端口[主要用于 Telnet(远程登录)服务,是 Internet 上普遍采用的登录和仿真程序],并记录这个端口的活动情况。当一个黑客探测到这个虚拟的 Telnet 服务时,就会试图开启一个登录对话,虚拟 Telnet 服务进程就会对他的请求给予响应,而配置在诱骗系统中的信息捕获工具会记录下黑客的所有活动。虚拟诱骗系统也可模拟成某个具体的操作系统,比如它可以伪装成一个正在运行的 UNIX 操作系统,向外提供 DNS 服务。虚拟诱骗系统最大的优点就在于设计和维护的简易性,设置它们仅仅需要选择操作系统、安装所要模拟功能的仿真软件,以及设置信息捕获程序等操作,它使得黑客不能够真正地侵入系统,或者再利用它去破坏其他网络系统。然而对于虚拟诱骗系统来说,又存在不足。一是它只能诱骗初级黑客。由于虚拟诱骗系统并没有一个真正的作业系统来支撑,所以经验丰富的黑客会发现很多命令在主机中不起作用,他会立即意识到进入的只是一个虚拟环境。二是虚拟诱骗系统能够捕获记录的入侵信息种类有限。例如,一个伪装成 FTP 服务器的虚拟诱骗系统,就只能捕获和 FTP 相关的入侵信息。三是一旦黑客进行了虚拟诱骗系统没有预料到的破坏行为后,系统将无所适从,这时大部分的虚拟系统都会产生一个报错信息。

真实诱骗系统则都使用真实的操作系统和服务程序。我们可以在一台真正的 UNIX 操作系统上运行真正的 FTP 服务进程,当一个黑客主动地入侵到真实诱骗系统中时,虽然他们自己还不知道已经落入陷阱,但是他所做的一切行为都已被记录下来。为此,需要在真实系统中配置可靠的记录程序来记录黑客的入侵行为。与此同时,真实系统需要设置一个防火墙来防止黑客利用入侵本系统来攻击其他无辜网络系统。真实诱骗系统具有两个明显的优点:一是通过让黑客攻击真实系统,可以捕捉到更多真实的入侵信息,了解他们的入侵技术和思想。二是由于真实诱骗系统对黑客的行为没有任何预先的猜测,所以它需要如实地记录对于系统的任何操作,这也能够使我们学习到许多更新的入侵技术。然而,真实诱骗系统的缺点是它有可能被黑客攻破后从而变为侵入其他正常网络系统的跳板,增加了网络中正常网络系统的安全风险。为了防止这种情况发生,需要在真实诱骗系统所在网络与正常网络之间架设防火墙,以限制二者间的信息流向。

为了增加网络诱骗系统伪装的真实性和可信性,通常认为一个功能强大的诱骗系统中应该既要有 Windows,又要包括 Linux、UNIX 等多种操作系统;既要部署虚拟诱骗系统又要配置真实诱骗系统;既要有优秀的信息捕获工具又要有良好的访问控制机制。网络诱骗系统的拓扑结构如图 3-17 所示。

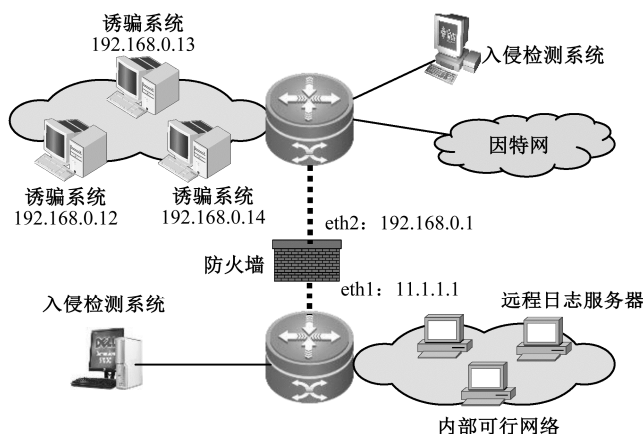


图 3-17 网络诱骗系统的拓扑结构

### 3. 基本要求

为了有效地使用网络诱骗技术，同时不干扰其他实际系统的正常工作，网络诱骗必须满足下列的基本要求。

(1) 安全性。诱骗技术必须保证自身的安全性，同时不能对宿主计算机或所属网络环境引入新的安全问题。

(2) 无干扰性。诱骗技术必须能够适用于所属的网络环境，且与其他实际的系统、服务协同工作，在自身运行时不影响其他系统和服务的正常运行。

(3) 隐蔽性。诱骗技术必须有一定的迷惑性，使攻击者在攻击的过程中无法发现是在攻击诱骗系统。在较为高级的诱骗系统中，即使攻击者占领诱骗系统，攻击者仍然无法发现所攻击的系统是诱骗系统。

(4) 可追查性。诱骗技术必须适当地记录攻击过程，从而保证能对攻击过程进行追踪回放，例如记录攻击者的 IP 地址、攻击时间、击键记录等。

### 4. 网络诱骗技术

#### 1) 蜜罐

蜜罐是出现最早的诱骗技术。作为一种安全资源，蜜罐伪装成真实的目标系统来诱骗攻击者对其进行攻击。蜜罐的主要目标是容忍攻击者入侵、记录并学习攻击者的攻击工具、手段、动机和目的等行为信息，尤其未知攻击的行为信息，从而调整网络的安全策略，提高系统的安全能力。同时蜜罐还具有转移攻击者注意力、消耗其攻击资源和意志的作用，因此，可以间接保护真实的目标系统。目前，常见的蜜罐包括 BOF (Back Officer Friendly)、Specter、Honeyd 和 ManTrap 等。

使用蜜罐作为网络诱骗技术，可以不依赖任何的检测技术判定攻击者的行为，因此可减少网络攻击的漏报率和误报率，而且能够收集新的攻击工具和攻击方法，而不像目前的大部分入侵检测系统只能检测已知的攻击行为。

## 2) 蜜场

蜜场是一种集中式的网络诱骗技术。蜜场中部署大量的蜜罐系统，通过子网内设置一系列的重定向器，间接地接受子网转发的网络攻击，其概念关系如图 3-18 所示。蜜场的主要目的是在大型分布式网络中简便地部署和维护蜜罐，对各个子网的安全威胁进行集中收集。子网中设置攻击检测器，若检测到当前的网络数据流是网络攻击时，则通过重定向器将这些流量重定向到蜜场中的蜜罐主机上，并由蜜场中部署的数据捕获和数据分析工具对攻击行为进行收集和分析。

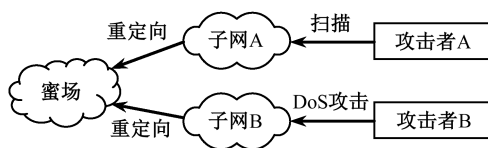


图 3-18 蜜场的概念关系

蜜场的优越性在于其集中性，使得其部署变得较为简单。蜜场可以作为安全操作中心的一个组成部分，由安全专业研究和管理人员进行部署和维护。蜜场模型的集中性也使得蜜罐的维护、更新、规范化管理及数据分析变得较为简单。此外，将蜜罐集中部署在蜜场中还减少了各个子网内的安全风险，有利于对引入的安全风险进行控制。

## 3) Honeytoken

Honeytoken 是最简单的诱骗技术，基本思想是攻击者的目标不仅仅在于攻陷网络和主机本身，往往更多时候是对信息内容的攻击。因此，在系统中设置一些正常情况下永远不会使用的信息内容（称为 Honeytoken）作为诱饵。一旦发现这些 Honeytoken 被访问，则预示攻击者可能对信息内容发起攻击，从而可以发现并追踪攻击者的攻击活动。较容易实施的 Honeytoken 包括数据库中的某些无用数据项，系统中故意设置的弱口令账户等。

## 4) 蜜网

蜜网是复杂、高效的诱骗技术，其主要目的是收集黑客的攻击信息。蜜网的实质是高交互的蜜罐系统，但与传统蜜罐的差异在于，蜜网构成了诱捕网络架构体系，在这个架构体系中可以包含一个或多个蜜罐，同时保证了网络的高度可控性和高逼真性，并可以提供多种工具对攻击信息进行采集和分析。虽然蜜网可以提高诱骗系统的检测、响应、恢复和分析的能力，但配置蜜网需要的硬件代价和管理代价也明显高于其他诱骗系统。

## 5. 重要信息捕获的方法

一个设计出色的网络诱骗系统，即可以诱骗黑客攻击自身又能够及时记录入侵者的行为，以达到间接保护真实网络系统的目的。

首先，诱骗系统伪装的真实性。它能够迷惑入侵者，使他误以为所攻击的诱骗系统就是一个真正的网络系统，并且不能让黑客察觉在诱骗系统中存在着各种记录手段。这样，

黑客才会攻击它，达到我们记录、学习、提高的目的。

其次，网络诱骗系统中的信息捕获手段应该是多层次的。网络诱骗系统中的信息捕获能够获得所有黑客的行动记录，这些记录最终将帮助我们分析他们所使用的工具、策略以及攻击的目的。以下列举了几种重要信息捕获使用的方法技术。

(1) 利用防火墙的日志功能。防火墙不仅可以记录下所有的进入及流出网络诱骗系统的连接企图，而且还能及时发出警告信息，在必要时阻止黑客的攻击行为。

(2) 利用入侵检测系统的日志功能。入侵检测系统能够检测出所有入侵行为并且如实地记录下来，另外它还能在发现一些可疑举动的时候向管理员发出报警。在诱骗系统中，入侵检测系统可以用来对特定的一些连接进行细节信息的收集捕获。我们使用的入侵检测系统可以是一个免费的数据包嗅探器 **Sonrt**，它能捕获所有在网络中传输的信息，进入或流出诱骗系统的数据包都将被记录到它的日志文件中。同时，可以在诱骗主机上配置击键记录程序，将黑客所进行的击键记录写入指定的目录文件中，这些都将秘密安全地传送到远程日志服务器上。

(3) 利用操作系统自身的日志功能。当然，我们不能仅仅在本机上保存日志文件，而应该及时地将系统日志传送到远程日志服务器上。在多数的 UNIX 机器上，可以简单地在系统日志文件的配置中加上一条远程日志服务器的条目来完成日志传送功能；而在 Windows 机器上，一般需要配置第三方的远程日志记录工具，将日志文件写入共享的远程日志服务器上。

## 6. 网络诱骗系统的体系结构

网络诱骗系统的体系结构如图 3-19 所示，由初始配置模块、诱骗模块、接收处理模块、管理中心模块和数据库模块组成。图 3-19 显示了这五个模块之间的逻辑关系。这些模块可以处于同一台主机中，也可以处于不同的主机中。其中初始配置模块、接收处理模块和诱骗模块（图中虚线框中的模块）是组成诱骗主机的主要模块。一个诱骗系统可以由多个诱骗主机组成，诱骗主机可以部署在互联网的任意位置。管理中心对这些诱骗主机进行统一的管理和配置。

可扩展诱骗系统首先由管理员通过管理中心发送控制信息对各个模块进行初始化配置，确定诱骗系统的工作方式。这些控制信息通过相应的通信协议传送到各个模块中。然后，诱骗模块以配置文件中定义的方式启动系统，开始侦听、捕获和解码所有来访的数据包。与此同时，将解码的数据包与规则库中的规则进行匹配，并按照匹配结果对不同的攻击类型进行相应的输出响应。诱骗模块产生的警告和日志等信息通过响应输出传送到接收处理模块，经转换后送到管理中心。这些信息一方面以指定的方式存储到数据库供统计分析之用，另一方面发送至控制终端，进行实时监视和控制。

(1) 初始化配置模块。系统的启动内容和诱骗规则是通过初始化配置模块完成的。管理员通过设置配置文件和规则库决定诱骗系统的工作方式。配置文件决定系统的启动参数，如系统模拟何种操作系统环境和哪些服务、系统是否延迟响应、系统日志记录类型和路径，以及发送警告的类型和路径等。



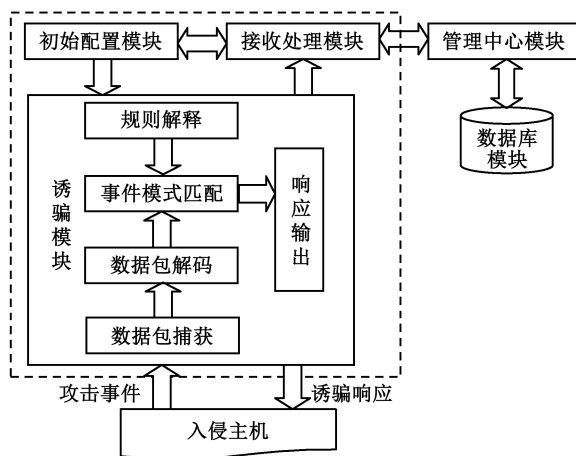


图 3-19 网络诱骗系统的体系结构

(2) 诱骗模块。该模块是诱骗系统的核心模块，由数据包捕获、数据包解码、事件模式匹配、规则解释和响应输出五个子模块组成，其结构可参见图 3-19。它完成网络数据包的捕获、解码、匹配、响应和发送等各项功能。当诱骗模块按照初始配置模块确定的诱骗方式启动后，首先由规则解释子模块对规则库中所描述的规则进行解析，形成系统容易处理的规则链表和数据结构，并将其送到事件模式匹配子模块中。同时，由数据包捕获子模块对当前网络访问进行监听，捕获来访的数据包并将其送至解码子模块进行解码。按照原始网络数据所属的网络协议，解码子模块将其解码为相应的分组数据结构，并将该解码后的协议分组信息提交事件模式匹配子模块处理。事件模式匹配子模块对已解码的网络数据进行分析，与规则库中描述的每一事件特征进行比较，在发现网络数据含有某些攻击事件的特征标志时，通知响应输出子模块处理。响应输出子模块根据事件模式匹配子模块提交的事件类型、规则库中所指定的响应动作和响应方式向入侵主机发送诱骗响应数据包，并向管理中心发出告警信息和进行日志处理。

(3) 接收处理模块。该模块是管理中心模块与诱骗模块和初始配置模块之间的桥梁。它的主要功能包括两方面：一是接收来自诱骗模块的数据，进行整理和协议转换，并发送到管理中心；二是负责把管理中心传来的控制信息经协议转换后传送到初始配置模块。在诱骗系统初始配置时，管理中心采用安全通信协议向接收处理模块传递控制命令（如静态配置、启动、停止等命令），接收处理模块根据命令的内容进行相应的格式转换，并通过进程通信执行这些命令。诱骗模块在运行过程中检测到攻击事件后，将告警、日志、捕获时间、原始数据包等信息提交给接收处理模块。接收处理模块在进行格式转换等处理工作后，利用安全通信协议将它们传给管理中心。

(4) 管理中心模块。管理中心是诱骗系统的人机界面，是网络管理员对整个诱骗系统实施管理和配置的场所。管理中心负责对管理员输入的命令信息进行初步的检验，并将正确的命令传送给接收处理模块。与此同时，管理中心模块也接收告警、日志等接收处理模块提交的信息，并对这些信息进行显示、存储等处理工作。另外，管理中心模块还应具有

数据库管理和数据统计分析功能。管理中心对分布在多个子网上的诱骗主机进行集中管理，一台管理主机可以配置和管理所有的诱骗主机。

(5) 数据库模块。数据库应采用成熟安全的大型数据库系统（如 Oracle 数据库等），其功能是存储诱骗系统的所有日志信息和告警信息，以供管理中心进行信息查询和统计。

## 7. 美军的网络诱骗系统

2002 年 8 月，美国空军第 100 通信团演示了先锋型的网络诱骗系统，它由两套防卫性系统构成，功能是探查、追踪和确认潜在的网络入侵者。他们共同演示了制造虚拟网络（虚假的计算机设备）的军事价值。虚拟网络被用来当作陷阱，它诱使敌人进攻并从中获益。网络诱骗系统是建立的一个虚假网络，它在系统管理员不知情时向其通报敌军已经入侵了网络。系统的作用并不只是探查黑客，它还可以让系统监测人员跟踪黑客行动，并让其最终进入陷阱。网络诱骗系统以深度结构增加了网络安全的可靠性，给美国空军带来了保障信息与数据安全的新能力。它是美国空军在网络空间作战中制服内外入侵者的新武器。

### 3.5.3 网络攻击预警系统

#### 1. 概述

网络攻击预警是指针对网络上已经发生的或即将可能发生的网络攻击事件进行检测并告警。其通过使用各种有效的方式，分析不同安全设备采集到的网络安全事件来预测网络安全态势和网络攻击事件。

网络攻击预警以入侵检测技术为源数据采集的方法，通过采用高速报文捕获与存储、数据缩减、数据清洗、数据关联、数据挖掘、数据融合、可视化、应急防护等技术，发现潜在的攻击行为特征或新的攻击模式，根据流量分析、网络运行监控、病毒威胁、威胁关联分析、告警数据聚集分析等方法，预测潜在的或已经发生的网络攻击事件并发出警告，以便采取有效的防护措施。

网络预警技术的研究内容主要包括网络入侵技术、检测模型、审计分析策略、网络威胁态势分析、告警关联分析等。通过入侵检测采集网络威胁数据，依据各种检测模型从海量的威胁数据中找出真实的攻击事件或攻击前兆，使用有针对性的统计、审计分析策略检测未知的攻击模式和隐藏的攻击行为。通过这些技术的有机结合，形成一个互动发展的整体。

由于网络的危害行为是一系列的很复杂的活动，特别是有预谋、有组织的网络入侵，因而有效的预警和响应技术在实现上比较复杂并有很大的难度。预警的复杂性表现在对攻击发现、来源识别和企图判定等方面，响应的复杂度则体现在危害程度和潜在能力的判断、网络跟踪、攻击前防护等方面。

## 2. 系统需求分析

网络攻击预警系统的功能需求如下：

- (1) 实时网络数据流跟踪：对监控的网络，实时监测网络上的数据流。
- (2) 网络攻击模式识别：通过某种方法，比如建立已知的网络攻击模式数据库等，从网络数据流中发现网络攻击模式。
- (3) 网络安全违规活动捕获：能够根据用户自定义的网络安全策略对网络活动进行检查，捕获网络安全违规活动。
- (4) 对将要发生或已经发生的网络攻击进行预警：通过某种攻击预测算法从IDS告警数据中挖掘出潜在的威胁或将要发生的攻击，以便进行有效的防御。
- (5) 对攻击的下一步动作进行合理的推断：通过发现对潜在的威胁或前期攻击动作，使用某种算法，对攻击的下一步动作做出合理的推断。

系统不仅要有上述功能性需求，也包含以下必要的非功能性需求：

- (1) 系统自身安全：要求实现自身的数据传输的保密性、完整性、可用性。系统在传输数据的同时，需要保证自身的数据不被影响。系统自身能承受一定的网络攻击，架构和实现上不能留有明显的漏洞。
- (2) 稳定性：系统可以长时间稳定地运行，在出现故障时可以有效地自我恢复。
- (3) 性能：要求采集达到实时性，能够反映当前网络的安全形势。由于攻击预测是为了防范，实时地发现攻击前兆并提出预警，才能支持迅速采取有效的防御行动。

## 3. 系统流程结构

为了便于描述，先给出网络攻击预警系统整体的模块划分，如图3-20所示。

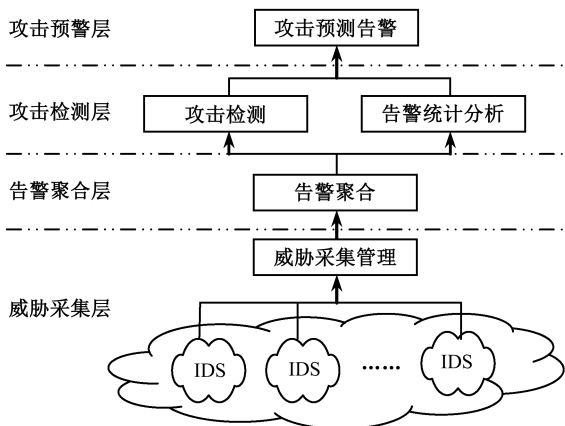


图 3-20 网络攻击预警系统整体的模块划分

网络攻击预警系统总共分为四层。分别是威胁采集层、告警聚合层、攻击检测层、攻击预警层。每一层完成攻击预警整体流程中的一个阶段的功能，收集分析下一层的数据，

并将分析后的结果数据发送给上一层。

网络攻击预警的目的就是从网络安全事件中发现攻击前兆或攻击历史，并发出报警。其处理的数据源主要是网络安全事件和网络数据流。网络安全事件主要是由 IDS 进行采集，即 IDS 检测网络中可能的威胁数据包并发出告警。网络数据流则是通过监控网络各种数据流的变化来检测网络运行状态。其输出的预警是可能即将发生的网络攻击事件或已经发生的网络攻击事件。对可能发生的攻击事件，需要给出可能的攻击方式、攻击目标、攻击源等信息。

部署在被保护网络中关键节点上的 IDS 负责采集网络中的安全事件，并汇总到威胁采集层。威胁采集层对 IDS 汇报的告警事件进行标准化处理并做简单的过滤，然后将告警上传给告警聚合层。威胁采集层的任务主要在于统一管理所有的 IDS 工具，协调各个 IDS 的一致工作。告警聚合层对从威胁采集层收集来的告警数据通过各种聚合算法聚合，提升单个告警的有效信息含量，同时也过滤掉无效的告警。告警聚合层通过对威胁采集层来的海量告警进行清洗，去掉大部分的无效告警数据后，可以方便上层的攻击检测层进行复杂的实时攻击检测。因为攻击检测算法的复杂性，如果数据量过大，会无法满足实时的要求。攻击检测层对清洗过后的告警使用不同的攻击检测算法，挖掘出隐藏在海量低层简单告警中的高层攻击场景数据。攻击预警层使用攻击检测层挖掘得到的网络攻击信息进行提炼，将攻击预警需要的攻击方式、攻击目的、攻击源等信息总结出来，同时提供接口以便后期的攻击响应操作。

#### 4. 系统功能结构

在将网络攻击预警系统分为四层的基础上，针对每一层的功能需求先给出每一层的具体功能和不同层之间的数据流，然后给出系统功能结构图。

威胁采集层，包括分布于受保护网络的关键节点上的 IDS、IDS Agent 和 Agent Manager。IDS 负责采集网络中的安全事件。IDS Agent 负责将原始的 IDS 数据进行简单的过滤并转换为所定义的标准威胁描述格式。Agent Manager 负责管理所有的 IDS Agent，支持 IDS Agent 的添加、删除、崩溃恢复、启动、停止、重启等操作。

告警聚合层，主要负责对告警数据进行聚合，主要是对重复告警、并发告警进行合并，对告警进行分类，另外安装定制的不同的聚类方法对告警进行聚合。告警聚合的目的第一是为了去除大量的无效告警，以支持实时的告警关联分析；第二是通过聚合发现某些攻击模式的网络攻击。

攻击检测层，主要负责从上报的告警中挖掘出隐藏的攻击行为，并将检测结果传给攻击预警层。攻击检测层的检测方法可以有多种，可以方便地加入或删除某种检测手段。目前包含：扫描/发现类攻击检测、DoS 及 DDoS 攻击检测、告警关联分析、网络威胁态势分析、网络威胁数量统计分析等方法。由于网络攻击的方式多种多样，针对不同的攻击方式，使用单一检测手段是较难达到目的的。通过对一些特定的攻击使用特定的检测手段可以有效地提高查全率、查准率。

攻击预警层，主要负责根据攻击检测层分析得到的网络攻击事件的预测数据进行攻

击预警。综合使用攻击检测层分析得到的可能发生或已经发生的网络攻击场景，提炼出已经发生和可能即将发生的网络攻击的详细信息，同时提供数据接口以便进一步的预警响应处理。

在系统整体大的框架下，每一块又是由多个部分组成的，网络攻击预警系统整体的系统功能结构图如图 3-21 所示。

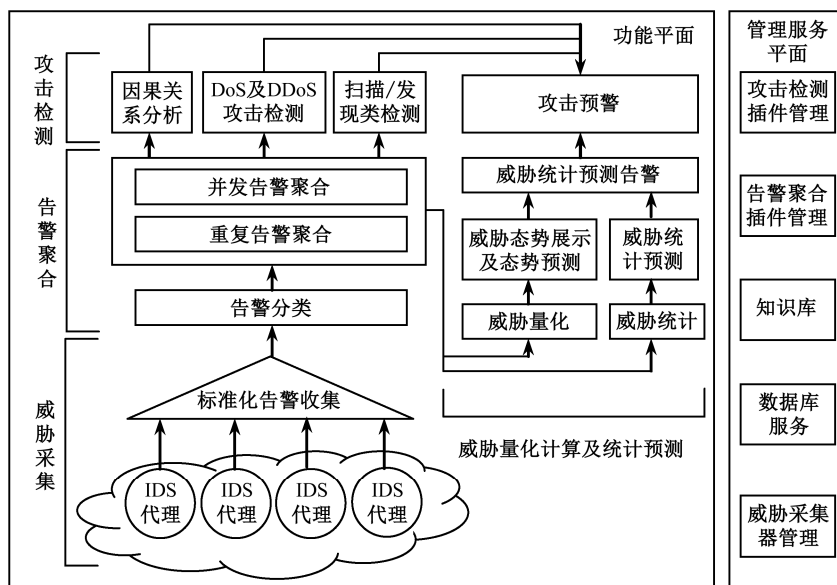


图 3-21 网络攻击预警系统整体的系统功能结构图

## 5. 美国计划建立网络攻击预警系统

美国高级情报研究计划署（IARPA），隶属国家情报总监办公室，负责执行各类“高风险+高回报”研究计划。2015年8月，该机构计划开展网络攻击预警研究，旨在结合内部预警系统和外部预警系统，打造名为“网络攻击非常规自动化检测环境”的网络安全威胁自动预警系统，自动检测网络攻击行为。该系统具有非常规性、自动性、高质量性的特点。

如今，网络攻击预警系统皆以常规感应（内部感应）数据为主要攻击情报来源。常规感应（内部感应）是指，在用户组织内部安装感应装置，预警系统主要根据常规感应装置对内部网络的监测，对比漏洞、病毒、攻击特征等网络安全事件数据库，进行有针对性预防。

IARPA 希望打造的“网络攻击非常规自动化检测环境”系统，旨在以非常规方式自动对网络威胁进行预警，并将网络威胁的预测提前至攻击发生的几小时甚至数周之前，若成功，将是网络攻击预警方式的一大变革。该计划于 2016 年开始，研究成果将在 3.5 年内完成。

### 3.5.4 其他的防御武器简介

#### 1. 网络盾牌

网络盾牌（CyberShield）是美国国家安全局正在筹备建设的一种大规模网络安全防御系统，用于抵御敌方针对美国关键基础设施所进行的各种网络攻击。网络盾牌系统可以实时分析网络中的数据包，侦察各种可能的入侵甚至攻击行为，并随时记录各种事件。如果受到攻击，网络盾牌系统可以立即启动强大的实时防御系统，迅速滤除各种非法数据包及其他攻击载荷；如果无法排除威胁，网络盾牌系统可以申请启用物理隔绝机制，并将威胁行为上报，以待进一步处理。

美军的网络盾牌重点建设三层网络防御体系：第一层，常规性保护；第二层，部署新的入侵侦察和检测系统；第三层，部署新的、包括国家关键设施的网络域态势感知系统，可高度融合美国和欧洲战略资源并安全可信地共享，为主动防御提供技术基础和联合行动的手段。

#### 2. 网络攻击告警系统

为保证网络安全，美国国防信息系统局（DISA，Defense Information Systems Agency）计算机应急响应工作组使用网络攻击告警系统——深查威胁管理系统和深查告警服务系统，以获得计算机系统自身脆弱性及遭受威胁情况的报告。这两种新软件可以对潜在威胁做出告警并推荐相应的反应手段。深查威胁管理系统从全球 180 多个国家的 19 000 多家公司的防火墙和入侵检测系统收集攻击数据，然后向 DISA 提供最新的安全信息，并定期进行情况更新。深查告警服务系统汇集了 1600 多家供应商和 3200 多种产品在安全性方面的弱点后，通过电子邮件、传真和短消息等方式为美国 DISA 发送告警。

#### 3. 网络漏洞扫描仪

网络漏洞扫描仪可以对所扫描的网络漏洞进行分析，提示每个漏洞可能受到攻击的危险级别及相应堵漏方法，以防计算机恐怖活动、病毒和其他威胁。美国陆军已选定哈里斯公司的 STAT 漏洞扫描仪作为网络空间的防御武器。STAT 扫描仪能分析所扫描的漏洞，提示每个漏洞可能受到攻击的危险级别，以及相应的堵漏方法。美国陆军使用 STAT 扫描仪监测其在全球的工作站和服务器，对各地网络的弱点提供详细报告。

#### 4. “网络狼”软件代理

“网络狼”是一种分布式网络攻击智能嗅探软件，可实时收集、记录来自遥感器、软件等入侵数据，自动处理和审查、提取入侵图样并发出报告。此外，它还可以把误警、虚警降至最低程度，从而提高系统管理效率。

5. 网络控制系统

网络控制系统负责美国空军网络空间防御，是空军战斗信息传输系统网络防御能力的主要组成部分。由于战斗信息传输系统构建了一个网络空间，但存在各种网络漏洞、易受网络攻击等缺点，网络控制系统就作为一种专用系统，通过各种手段、技术、软件等实现战斗信息传输系统的网络防御，确保美国空军战斗信息传输系统的安全。美国战斗信息传输系统概况见表 3-4。

表 3-4 美国战斗信息传输系统概况

名 称	战斗信息传输系统
负责机构	美国空军电子系统中心
系统组成	传输系统、网络防御系统、网络管理系统
总价值	64 亿美元
项目管理方式	无组织采购类型（ACAT- I ）（最初方式）； 分段管理方式（更改后的方式）； 信息传输系统：所有信息传输所需要的光纤、铜传输线、无线组件； 空军网络：建立、管理及保护固定网络的所有工作； 其他部分采用 ACAT-III 管理方式

网络控制系统之所以受到美国空军高度重视，是因为其可以为美国空军基地提供从有线到无线、从近距离到远距离的网络空间环境，可以为全球范围内的美国空军基地提供 IT 基础设施和信息传输，也可以为全球信息栅格环境下的美国空军提供企业级的网络管理和防御。

3.6 网络空间支援武器

作战支援类网络武器主要为网络空间对抗及网络武器的开发、测试、评估、采办等方面提供支持和保障。本节主要介绍网络空间的漏洞评估和网络空间安全态势的评估。

3.6.1 网络空间的漏洞评估

1. 基本概念

在网络空间安全中，“漏洞”一词被用来表明系统所存在的缺陷，在系统设计、实现

或操作管理过程中，这一缺陷可以被攻击者加以利用，以破坏系统可用性、完整性、一致性、可控性、可靠性和机密性，从而破坏系统的不可侵犯性。漏洞是导致系统安全性变弱的软件缺陷，或者部署不当导致系统产生的安全状态变迁。攻击主体能够利用这些缺陷通过已授权的手段获取对未授权资源的访问。

漏洞评估主要是利用漏洞信息评估漏洞对网络安全带来的风险，是鉴别、量化并优化系统中安全漏洞的过程。目前对漏洞评估主要集中在漏洞的探测和发现上。漏洞评估通常由加强版的网络扫描器执行。使用某些类型的自动化扫描产品可以探测某个 IP 地址范围内的端口和服务。大多数这样的产品可以测出所运行的操作系统和应用软件的类型、版本、补丁级别、用户账户和运行的服务。检测结果将会与所用产品数据库中的对应漏洞进行匹配。最终将得到一堆报告，其中会列出每个系统中存在的漏洞和可降低风险的相应措施。

2. 漏洞产生的原因

出现漏洞的原因可能有：密码防护能力弱，软件本身错误，软件调试不当，计算机病毒，源代码注入或结构化查询语言（SQL，Structured Query Language）注入类等恶意软件；在分析阶段，缺乏风险分析，存在未预见的风险；在设计阶段，依赖不安全的抽象层，在安全性与易用性或功能性间折中，缺少日志记录，存在残留风险；在实现阶段，没有检查输入参数，存在非原子检查，访问控制验证、不安全的异常处理；在配置阶段，存在软件的重用，复杂或不必要的配置，默认配置的安全性；在维护阶段，存在特征冲突或向后兼容性。可以说，漏洞无时无刻不存在。

漏洞的活动情况如图 3-22 所示，分为漏洞的来源、漏洞产生的时间、漏洞存在的位置。

漏洞的来源	故意	恶意	特洛伊木马	不能复制
				能够复制
			陷门	
		逻辑/时间炸弹		
		非恶意	隐秘通道	存储
	定时			
	其他			
	无意		校验错误	
		范围错误		
		串行错误		
		认证/鉴别错误		
		边界条件错误		
		其他可利用的逻辑错误		

漏洞产生的时间	开发期间	需求、规格、设计
		源程序代码
		结果代码
	维护期间	
	操作运行期间	

漏洞存在的位置	软件	操作系统	系统初始化	
			内存管理	
			进程管理	
			设备管理（I/O、网络）	
			文件管理	
			认证鉴别	
			其他	
		支持软件	特权程序	
			非特权程序	
			应用程序	
	硬件			

图 3-22 漏洞的活动情况

3. 漏洞的分类

常见的漏洞可分为以下几个类别。

（1）内存安全违例。它包括缓冲区溢出和悬挂指针等。



(2) 输入验证错误。它包括格式化字符串缺陷、SQL 注入、编码注入、目录遍历等。

(3) 竞争条件漏洞。它是攻击者通过构造竞争条件而产生的漏洞。比较有名的有 TOCTTOU (Time-Of-Check-To-Time-Of-Use) 漏洞和符号链接竞争漏洞。

(4) 权限混乱漏洞。典型的权限混乱的攻击有 FTP 反弹攻击等。FTP 反弹攻击是利用了 FTP 协议的 PORT 命令来让第三方的 FTP 服务器对目标主机进行端口扫描。

(5) 权限提升漏洞。这是一种可以让用户获得更多权限的软件缺陷，可以分为水平权限提升漏洞和垂直权限提升漏洞。

另外，按计算机因素的漏洞分类可参见图 3-23。

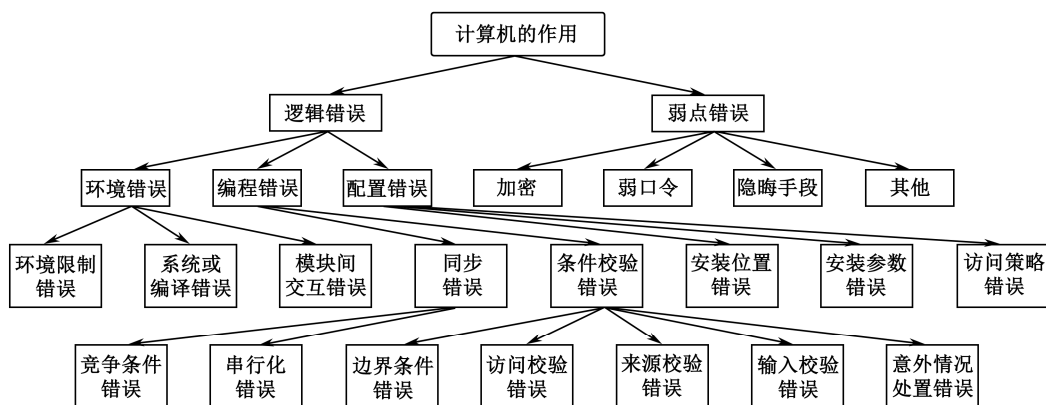


图 3-23 按计算机因素的漏洞分类

#### 4. 漏洞评估技术

漏洞评估技术主要涉及网络漏洞分析技术、漏洞发现预测技术和网络漏洞风险量化评估技术、基于规则的漏洞评估技术和基于模型的漏洞评估技术。

##### 1) 网络漏洞分析技术

网络漏洞分析是网络漏洞评估的基础。攻击者可以通过攻击一个漏洞获得攻击另一个漏洞的前提权限，从而形成一个漏洞利用链路，最后到达目标。网络漏洞分析技术就是要研究网络中的漏洞是如何相互关联的，并结合攻击者发起攻击的规律，预测漏洞被攻击者利用的各种可能性。

##### 2) 漏洞发现预测技术

漏洞发现预测是利用漏洞发现的历史数据预测未来一段时间发现一定数量和严重程度新漏洞的概率。漏洞发现预测技术主要有时间序列分析、线性回归分析和神经网络分析方法。不同的漏洞发现预测技术有不同的适用问题。

### 3) 网络漏洞风险量化评估技术

网络漏洞风险量化评估是利用漏洞信息量化漏洞对网络安全性的影响,根据一些评估标准,以及专家的知识经验等进行评估。通过对漏洞的研究分析,提取出能够反映漏洞危害的属性指标,建立好漏洞评价指标体系并量化处理,之后利用相关公式计算得出漏洞的风险值,定量反映漏洞的危害性。基于量化的漏洞评估技术能给出一个直观的评估结果,易于理解,但依据专家经验对大量漏洞评估,会导致工作量过大,且评估结果主观性较大。

### 4) 基于规则的漏洞评估技术

基于规则的漏洞评估是指根据发布的权威信息安全标准来定性评估漏洞,或对已发现的漏洞提取相关特征进行归纳总结形成规则表达式,从而对发现的新漏洞与之前发现的漏洞进行匹配,实现对安全漏洞的评估。基于规则的漏洞评估技术能够给出漏洞的危害等级,根据归纳总结的规则检测漏洞,只能对已发现的漏洞进行检测,但在检测潜在的新漏洞方面却存在不足。

### 5) 基于模型的漏洞评估技术

基于模型的漏洞评估技术是指利用收集到的漏洞信息,建立数学模型,分析系统被攻击后的所有可能存在的状态和行为,挖掘出潜在的漏洞或攻击路径,利用建立的状态图得到所有的可能攻击路径,实现对漏洞的评估。基于模型的漏洞评估技术能够有效评估整体网络的安全性,找出潜在的安全漏洞。攻击图、攻击树和特权提升等模型都是基于模型的评估漏洞技术中的一种应用。基于攻击图的分析方法就是分析不同攻击路径上利用漏洞的概率,以此分析攻击者成功到达目标节点的概率。

## 5. 漏洞评估系统体系结构

漏洞评估系统是指混合结构型运行期漏洞评估系统,既给出了对基于主机漏洞评估技术架构的支持,也给出了对基于网络漏洞评估技术架构的支持。系统在体系架构方面,必须考虑到以下事实:

(1) 在基于主机漏洞评估模式下,对主机的计算资源必须拥有管理员权限,因此系统宜采用客户机/服务器(C/S, Client/Server)结构。C/S结构应用的优点在于可以在主机范围内使用计算资源。

(2) 另外,为了系统有一个易于理解的可视化操作界面,系统宜选用浏览器/服务器(B/S, Browser/Server)结构。B/S结构型应用的优点在于不需要安装特殊的客户软件就可以对系统进行配置和管理。

(3) 一方面系统的处理能力(最大并发连接数、吞吐量等)终归是有限的,另一方面随着分支计算网络的不断加入,计算网络规模越来越大,为了提供足够能力的漏洞评估服务,系统宜采用分层多服务器结构。分层是为了方便对多服务器集中统一管理,多服务器

是出于系统负载的考虑,将客户业务分流至多个服务器以提高系统处理能力。

基于对上述事实的考虑,系统最终采用分层多服务器的混合结构体系,图 3-24 给出了漏洞评估系统的体系结构。

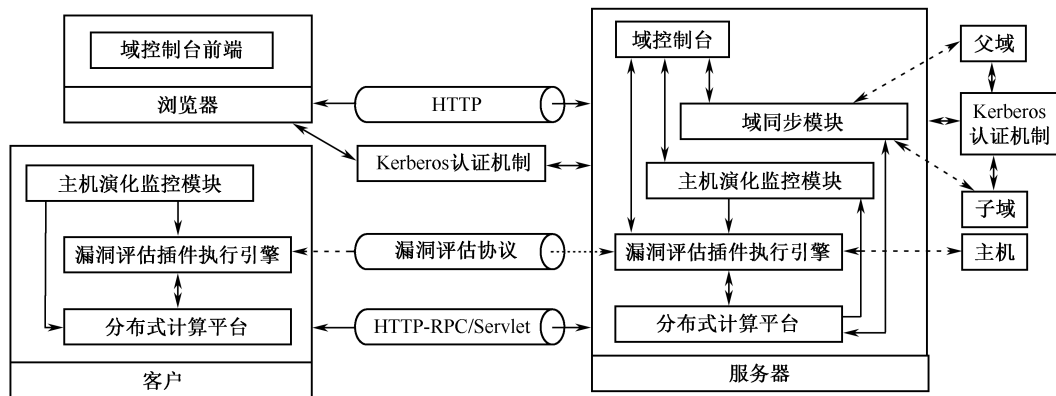


图 3-24 漏洞评估系统的体系结构

图 3-24 中虚线表示逻辑数据流,实线表示物理数据流。系统的组件分为客户组件和服务端组件。客户组件是指构成客户程序的组件。主要的客户组件有:

(1) 主机演化监控模块。该组件监控主机系统特征的变更和演化。若主机系统特征发生变化,主机演化监控模块会根据预置的漏洞评估方式来启动漏洞评估,若漏洞评估方式为服务端漏洞评估,则将所监控到的变化发送到服务器一端,由服务器进行漏洞评估,否则启动本地漏洞评估。

(2) 漏洞评估插件执行引擎。该组件执行实际的漏洞评估任务,其主要功能是保持插件完整性和执行插件。

(3) 分布式计算平台。该组件为系统提供基本的分布式计算能力,其主要功能是为客户端和服务端之间,以及服务器与服务器之间提供最基本的分布式计算服务,将通信功能设计从漏洞评估业务功能设计中分离出来。

服务器组件是指构成服务器程序的组件。主要的服务器组件有:

(1) 域控制台。该组件给出了服务器的管理接口,其主要功能是给出友好的人机交互界面,给出漏洞评估任务管理、漏洞库管理、域管理的图形化用户界面。域由服务器以及其所服务的客户,下级服务器组成,域与域之间以树型结构组成。域控制台给出了可通过浏览器对域进行管理的接口。

(2) 域同步模块。该组件给出了父域和子域之间的漏洞库同步功能以及服务器失效时的漏洞库恢复功能。

(3) 主机演化监控模块。该组件与客户端主机演化监控模块相对应,提供服务器端对主机演化监控的功能。

(4) 漏洞评估插件执行引擎。该组件与客户端漏洞评估插件执行引擎无论从结构还是实现上都是一致的。在客户端和服务端都维护一个漏洞评估插件,执行引擎的优势在于增强系统的灵活性,使得系统可以根据网络条件和主机条件自行选择,或者协商选择漏洞

评估方式。

(5) 分布式计算平台。该组件与客户端分布式计算平台功能相同。

另外，为了保障通信各方的身份安全和数据安全，系统还引进了 Kerberos 认证机制来确认通信各方的身份和对通信数据加密。

## 6. 漏洞评估业务流程

系统支持多种方式的漏洞评估：基于主机的漏洞评估，基于演化的漏洞评估，基于网络的漏洞评估。无论以何种方式进行漏洞评估，其基本原理，业务流程是一致的。漏洞评估业务流程如图 3-25 所示，分为漏洞评估计划制订、漏洞特征收集、漏洞特征分析和漏洞修复四个阶段。

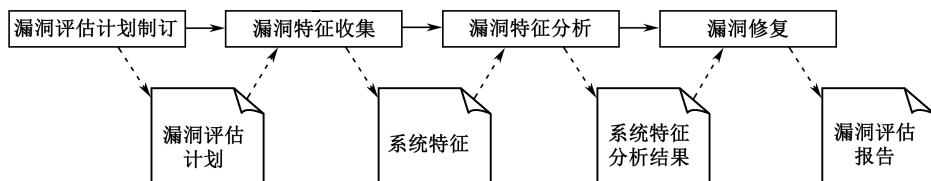


图 3-25 漏洞评估业务流程

(1) 漏洞评估计划制订阶段。该阶段负责制订漏洞评估计划，输出漏洞评估计划文件。

(2) 漏洞特征收集阶段。该阶段负责收集主机的系统特征，接收漏洞评估计划作为输入、输出系统的特征文件。

(3) 漏洞特征分析阶段。该阶段负责分析收集得来的漏洞特征，接收系统特征作为输入、输出系统特征分析结果。

(4) 漏洞修复阶段。该阶段负责修复评估结果为真的漏洞，接收系统特征分析结果作为输入、输出漏洞评估报告。实际上是在修复漏洞以后对之前输入的系统特征分析结果进行一次修订。

### 3.6.2 网络空间安全态势的评估

网络空间安全态势反映了网络过去和现在的安全状况，并通过对收集数据的研究处理来预测下阶段可能受到的威胁攻击，对网络运行状况有一个宏观的把握。网络空间安全风险态势评估是依据有关网络空间安全技术与管理标准，对网络系统及由其处理、传输和存储的信息的机密性、完整性和可用性等安全属性进行综合分析和评价的过程。它是风险管理的基础。通过风险态势评估，了解系统的安全现状，有针对性地采取安全措施，将风险控制可在接受的范围。

在评估中需要考虑以下问题：第一，对原始数据进行分析；第二，对数据的关联性进

行分析；第三，对网络空间安全态势的算法进行分析；第四，正确分析网络空间安全态势评估方法；第五，展现网络空间安全态势结果的技术成果；第六，将大量的数据进行相互融合，使得特征信息更加清晰；第七，减少数据的缓冲时间；第八，通过数据分析对未来可能出现的安全问题进行有效预防。

### 1. 网络空间安全评估分类

网络空间安全评估按照评估结果的实时性可以分为静态安全评估与动态安全评估。静态安全评估方法在评估时将评估的对象作为一个静止待评对象，不同的评估方法针对待评对象从不同的角度进行分析与评估，并给出整个对象的安全程度。传统的网络安全评估采用的都是静态评估方法，一般是在目标网络建成之初或进行大规模升级后对目标网络实施一次全面的评估。静态评估根据数据库中已知脆弱点和威胁信息来评估网络空间系统，这种方法的意义在于通过分析各种系统自身的安全性，反映系统由于设计或实现过程中的缺陷所产生的固有的安全风险，帮助开发建构更安全的系统。静态评估以脆弱性评估为重点，往往结合资产、威胁等因素，其中威胁频率大多采用历史统计数据。动态安全评估将待评对象作为一个动态变化的过程，针对动态过程中所呈现的安全相关特征建立相应的实时动态提取分析模型，通过连续的数据分析来实现对待评对象当前安全态势的评估。动态安全评估是一个较新的研究课题，也是当前网络安全领域研究的一个热点。

网络空间安全评估按照评估结果的形式分为定性评估和定量评估。定性评估是指对评估对象运用归纳与演绎、分析与综合等方法来对评估对象的各种因素及其属性进行分析处理。定性评估方法主要根据研究者的知识、经验、历史教训、政策走向及特殊案例等非量化资料对系统安全状况做出判断，一般通过调查的方式获取原始数据，然后通过理论推导演绎的分析框架，对资料进行编码整理，得出评估结论。定量评估是用数量指标来描述系统的安全状况，一般根据影响系统安全的各项因素的量值进行计算，但并不是所有的因素都可以用数字来表示的，而且各项因素之间的关系也难比较，同一因素在不同量纲中的值也不一样。定量的评估方法是用直观的数据来表述评估的结果，看起来一目了然，而且比较客观。定量分析方法的采用，可以使研究结果更加科学，更严密，更深刻。

### 2. 网络空间安全风险评估模块及其关系

#### 1) 静态评估模块及其关系

网络空间的安全风险评估，主要包括对来自网络空间外界的威胁评估和对网络空间自身资产评估两个模块。图 3-26 给出了网络空间安全风险评估模块及其相互关系。

图 3-26 中方框部分的内容是风险评估的基本要素，椭圆部分的内容是与这些要素相关的属性，也是安全评估要素的一部分。在对这些要素的评估过程中需要充分考虑业务战略、安全事件、残余风险等与这些基本要素相关的各类因素。这些要素在一定的时期内是稳定的，尽管通过多种方法进行分析，但均属于静态的，它不会通过网络行为的输入，而获得相对及时的响应，也就是说，没有包含动态分析的属性。因此，这些要素评估，属于静态评估模块的内容。

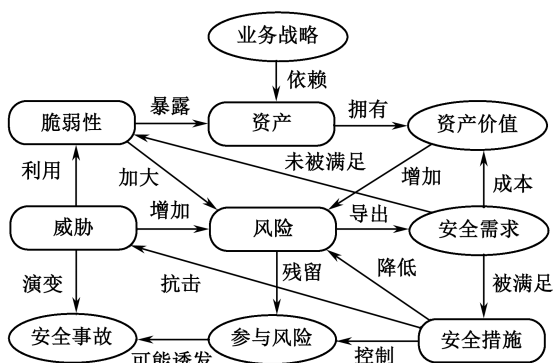


图 3-26 网络空间安全风险评估模块及其相互关系

## 2) 动态评估模块及其关系

动态评估模块在网络安全框架中是一个较为重要的角色，它弥补了静态评估模块中的不足。动态评估模块的特点是无法像静态评估那样找到准确的威胁对象和影响，也不关心资产本身的价值，但它可以通过对常态的数据进行收集，得到常态下的自我特征，可以检测到异常事件。

动态评估方法是从安全的实际出发，评估事件的正常和异常特性，不但可以解决由于未知所引发的不确定性，也客观地反映了系统当前所面临的实际威胁。动态评估各模块及其相互关系如图 3-27 所示。

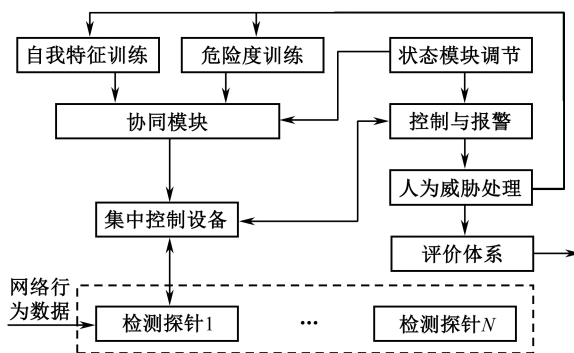


图 3-27 动态评估各模块及其相互关系

动态评估模块包括：自我特征和危险度训练建立动态特征库，模块对两种不同的检测方式通过打分机制协同二者的检测结果；网络的安全环境评估模块影响阈值的大小；集中控制设备对检测探针收集的网络行为、数据，进行捕获的结果分类和统一格式，并向检测探针发送控制命令，向控制与报警模块发送预警信息，并接收控制与报警模块的命令；预警信息通过人为威胁处理交给风险和成本评价体系模块进行评估，并通过风险和成本评价体系模块调整安全部署，人为威胁处理还将处理的结果反馈给自我特征训练模块，使得动态评估系统具有记忆特征。

自我特征训练是通过对正常行为的序列进行抽取,通过收集用户对业务的正常行为和管理员日常工作的正常行为而建立正常的行为序列,从中提取“自我”个体的表示形式。以用户视角和管理员视角分析,正常行为序列特征使得这些特征成为成熟的检测器。在检测过程中,比对被检测数据与正常行为特征的差异,从而评估这种差异是否属于未知威胁。对于危险度的训练,对不同的网络行为先天的危险度进行评价计算,对于各种网络行为在正常样本和异常样本中出现频率的分布不同,定义各种行为的危险度,再根据已知威胁状况获得阈值参数,并接受网络的安全环境对阈值参数的调节。

### 3. 网络空间安全威胁态势的评估流程

简单地说,静态评估模块就是通过对威胁和脆弱性的评估获得威胁库,根据威胁库建立可选安全方法库,再通过风险和成本评估模块选取部分合理的安全方法成为网络系统的实施安全方法。其流程见图 3-28 中虚线左侧部分。

网络空间安全体系中动态评估方法可采用基于统计的评估方法和基于人工免疫的异常事件检测和评估方法。这两种方法都是通过对对象的特性进行刻画,找到评估对象本质固有的特征表现,从而发现异常的事件,并将它们分析和呈现。其运作流程见图 3-28 中的中间虚线右侧部分。

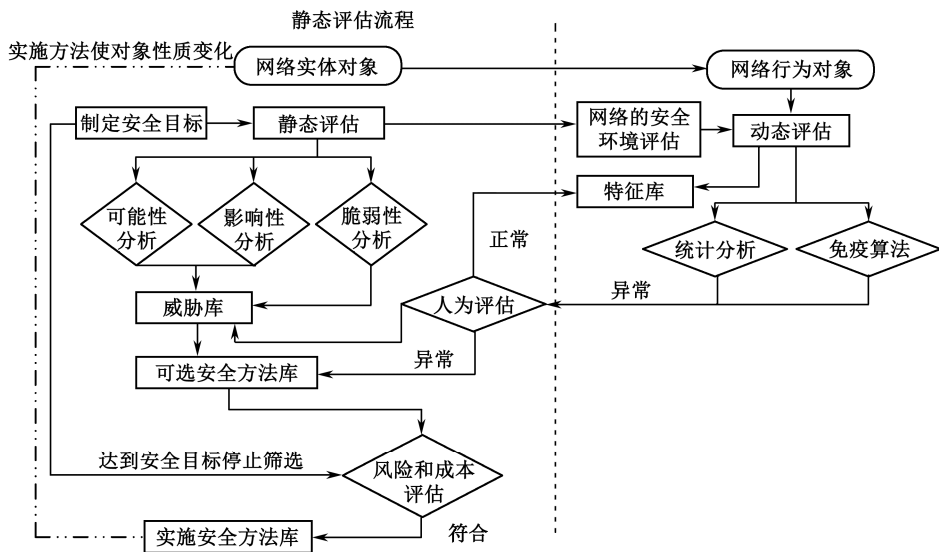


图 3-28 网络空间安全威胁态势的评估流程

### 4. 网络空间安全威胁分析

网络空间安全威胁可直接导致网络系统泄密事故。获取威胁信息的手段主要包括以下六种：（1）模拟入侵测试；（2）顾问访谈；（3）人工评估方式；（4）安全信息审计；（5）策略及文档分析；（6）入侵检测系统取样。对安全威胁进行分析主要涉及以下内容：（1）确定重要的信息价值及安全要求；（2）分析重要网络的薄弱部分并确定潜在威胁类型；（3）评估威

胁可以造成的实际损坏能力；（4）分析威胁成功攻击的概率；（5）推算遭受攻击所付出的代价；（6）根据攻击范围计算安全措施费用。

对网站进行安全风险评估，首先要确定网站面临的安全威胁。对于网站而言，主要的威胁来自组织外部的黑客攻击和内部人员的攻击。根据威胁来源的不同，在表 3-5 中列出一些主要威胁，并对威胁进行描述。

表 3-5 网站主要威胁列表

序号	威胁类型	威胁描述
1	操作失误	合法用户工作失误
2	权限滥用	合法用户利用自己权限破坏网站
3	权限提升	合法用户利用恶意手段提升自己权限
4	行为抵赖	合法用户否认自己的操作行为
5	假冒欺骗	非法用户使用欺诈手段获取敏感信息
6	篡改	非法用户未经授权更改网站信息
7	拒绝服务	非法用户利用拒绝服务手段攻击系统，导致网站无法提供正常服务
8	恶意指码	病毒、特洛伊木马、蠕虫、逻辑炸弹等感染
9	窃取数据	非法用户窃取网站的信息资源和敏感信息
10	物理破坏	非法用户对网站进行物理破坏
11	社会工程	非法用户利用社交等手段获取重要信息

5. 网络空间安全态势评估指标体系

1) 网络空间安全评估指标体系

要想建立一套科学、合理、实用、完善的指标体系，一般应遵循科学性、全面性、可操作性、系统性和层次性的指导原则。针对大规模网络空间宏观特性和复杂性，依据网络安全机密性、完整性、可用性、可控性等要求，给出了如图 3-29 所示的网络空间安全评价指标体系。

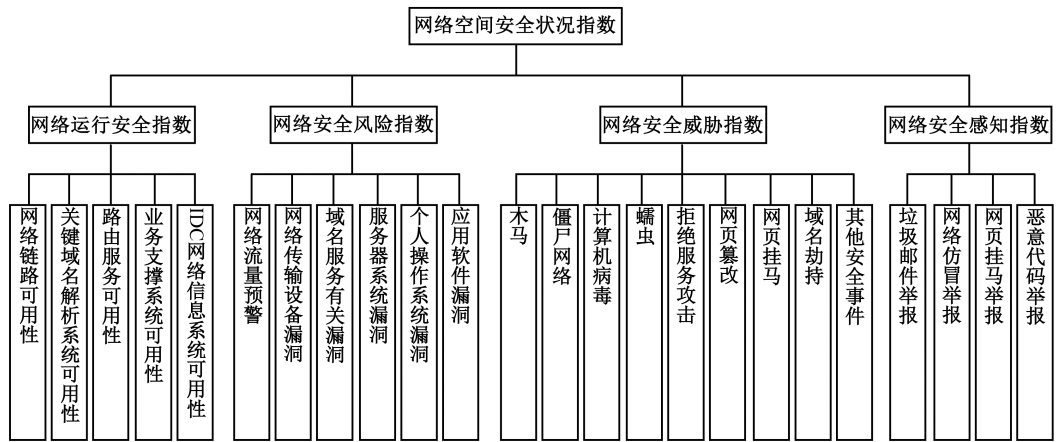


图 3-29 网络空间安全评估指标体系



网络空间安全评估指标体系主要从网络运行安全、网络安全风险、网络安全威胁、网络安全感知四个方面（一级指标）评估网络安全状况。这四个一级指标又由具体下级指标评估得到。网络运行安全主要反映网络链路、域名服务和路由等网络基础设施的当前运行状况；网络安全风险主要反映网络设备及系统当前所面临的风险，重点考察各种安全漏洞和骨干网络的流量异常情况；网络安全威胁主要反映互联网上已经发生的各类安全事件对网络安全的影响；网络安全感知主要反映用户对网络安全的感知，体现了网络安全对用户的影响。

## 2) 网络空间安全态势评估指标体系

在指标选取时综合考虑了不同层次（宏观网络、局部网络、主机、服务、攻击/漏洞），不同信息来源（流量、报警、日志、静态配置）和不同需求（普通用户、管理者、维护者），在指标组织时提炼出了四个表征宏观网络性质的一级综合性指标：脆弱性、容灾性、威胁性和稳定性，最后形成的指标体系。网络空间安全态势评估指标体系见表 3-6。

表 3-6 网络空间安全态势评估指标体系

一级指标	二级指标	一级指标	二级指标
脆弱性	网络漏洞数目及等级 关键设备漏洞数目及等级 子网内安全设备数目 子网内各关键设备提供的服务种类及其版本 子网内各关键设备的操作系统类型及其版本 子网内各关键设备开放端口的总量 网络拓扑	威胁性	报警数目 子网带宽使用率 子网内安全事件历史发生频率 子网内各关键设备提供的服务种类及其版本 子网数据流入量 子网流入量增长率 子网内不同协议数据包分布 子网内不同大小数据包分布 流入子网内数据包源 IP 分布
容灾性	网络带宽 子网内安全设备数目 子网内各关键设备的操作系统类型及其版本 子网内各关键设备访问主流安全网站的频率 子网内各关键设备提供的服务种类及其版本 网络拓扑 子网内主要服务器支持的并发线程数	稳定性	子网内关键设备平均存活时间 子网流量变化率 子网内不同协议数据包分布比值的变化率 子网内不同大小数据包分布比值的变化率 子网数据流总量 流出子网数据包目的 IP 的分布 子网内存活关键设备数目 子网平均无故障时间





# 第 4 章

## 网络靶场规划及其建设

随着网络空间攻防技术和武器装备的不断发展，建设能对网络空间进行安全技术验证和风险分析、对网络新技术进行评测、对网络武器装备进行研制试验和作战试验、对作战效能进行定量定性评估、对网络部队进行训练演练的网络靶场就愈发显得重要。确实，网络靶场已成为各国进行网络空间安全研究、学习、测试、验证、演练等必不可少的网络空间安全核心基础设施。世界各国均高度重视网络靶场建设，将其作为支撑的重要手段。目前，按照传统分类标准形成的靶场试验训练模式难以适应联合作战的现代化装备试验和部队训练的需要，设立专门的大规模的网络空间安全试验场所迫在眉睫。

### 4.1 概述



#### 4.1.1 建设网络靶场的必要性

目前，我国虽然高度重视信息安全保障工作，但仍有许多问题难以克服：真实网络攻防行动可能造成网络瘫痪和社会安全风险，现实网络环境难以完成网络攻防实验的具体要

求；有的网络信息系统属于关系国家安全和社会稳定的重要信息系统，如果在真实系统中进行测试和模拟攻防演练，将会使业务连续性遭受重大威胁。不仅如此，在真实环境中进行测试评估，人为干扰因素可能会令检测及攻防演练结果的真实性大打折扣，这就需要我国必须研究、建设接近真实网络信息系统环境的模拟仿真实验系统及技术，并尽早应用起来。

面对网络空间安全的发展与新趋势，为弥补差距、抢占先机、奋起直追、迎头赶上，我国必须瞄准关系全局和长远发展的网络空间安全领域，通过科学规划、顶层设计，深入推进机制创新、协同创新和开放创新，尽快启动网络靶场建设，提升我国网络空间安全核心能力。

通过网络靶场建设，可为金融、电信、能源、交通、电力等国家关键信息基础设施安全体系建设提供分析、设计、研发、集成、测试、评估、运维等全生命周期保障服务，解决无法在真实环境中对复杂大规模异构网络 and 用户进行逼真的模拟、测试和风险评估等问题，实现国家网络空间安全能力的整体跃升。

利用网络靶场可制订试验计划和配置方案，并提出各种安全管理制度，为技术人员提供现场技术支持服务。网络靶场可以支持多个并行或分段试验，试验结束时，靶场将释放分配的试验资源，由靶场完整回收并继续使用。

利用网络靶场，研究人员可以方便地设定主机、系统延迟、环境参数和敌方类型等内容，并立即投入试验。除了快速构建试验平台并节省试验时间，网络靶场还可以人为地使被测系统出现故障，然后重新启动系统再次进行试验。此外，通过自动设置过程，研究人员可以快速操作很多场景，开发出各种可能的新结构来应对威胁。网络靶场还可以进行网络态势感知，各种态势感知工具可以在靶场中进行测试以对比其性能。例如，可以测试一种信息安全优点和劣势，反馈给用户和研究机构，它还可以让用户改变传感器在网络中的位置，从而影响一个应用程序的态势感知。网络靶场还能够测试并评估网络复杂性。随着网络变得日益复杂，网络开始像生物系统一样对环境变化做出响应。靶场可以通过改变不同网络流量，使得技术人员更好地理解复杂系统中出现的异常。

网络靶场将彻底改革非自动化和测试管理的现状，支持大规模网络空间实验，为测试和证实新的网络研究技术和系统提供全自动的靶场和测试管理配套设施，为目前和未来的研究项目提供指导意见，为网络空间安全研究部门提供一种安全、革命性和全自动化试验环境，评估新的研究，加速技术更新，成为一个反复进行新型研究的试验场。

网络攻击是常见和不断增加的事件，维持一个强大的网络安全技术优势非常重要。针对真实的黑客攻击、电子对抗战术等网络空间作战方法构建实验环境，能为政府和军队提供逼真的网络空间虚拟环境，增强网络空间作战能力和提高国家安全保障水平。

鉴于上述存在的问题和网络靶场发挥的重要作用，我们应未雨绸缪，提前准备，学习美国的先进做法，尽快建立网络靶场，以应对我国网络设施中的薄弱环节和其他国家的网络威胁。

### 4.1.2 网络靶场的概念

网络靶场是为了应对网络信息技术与信息化武器装备的迅速发展，应对军事领域革命性的变化，适应信息化武器装备发展要求，通过模拟现代网络攻防战，提供近似实战的网络空间作战环境而建立的虚拟网络攻防演练平台。它针对不同操作系统的虚拟主机植入常见的网络攻击手段，观察靶场监控室，分析实验中收集到的数据，重现网络攻击对系统造成的破坏，针对各种破坏性攻击手段进行思考并应对，以达到强化网络安全防御能力的目的。

网络靶场可以为各种网络技术、攻击防御手段和制定的安全性策略和方案提供定量和定性的评估，实现信息系统和信息化武器装备的战术技术性能测试和作战效能评估，为网络空间作战和安全主管机构评估网络信息系统的安全程度提供一个可信性、可控性、可操作性强的演练和实验环境。

国家网络靶场是面向各类用户，涵盖各领域各行业典型应用的、军民结合的科研与试验保障环境，具有网络空间安全体系规划论证、网络安全防御技术演示验证和体系化安全性评估等能力。国家网络靶场的概念体系包括行业域、任务域和应用域三个层面，如图4-1所示。

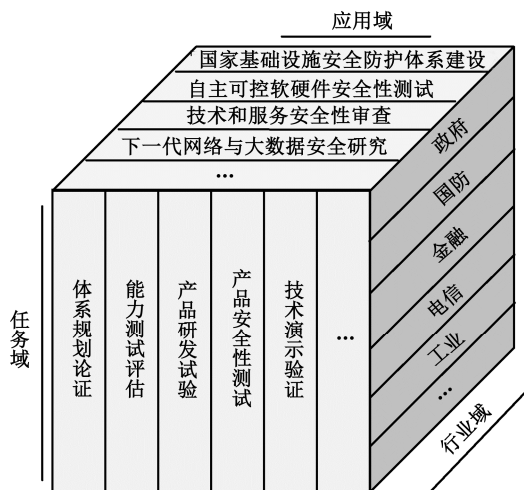


图4-1 国家网络靶场的概念体系

从行业域层面来看，国家网络靶场的核心是要涵盖政府、国防、金融、电信和工业等领域，满足其网络空间基础设施安全体系建设与科研试验应用需求。

从任务域层面来看，通过国家网络靶场的顶层设计与体系建设，可以完成网络空间安全体系规划论证、能力测试评估、产品研发试验、产品安全性测试、技术演示验证和人才培养等任务。

从应用域层面来看，国家网络靶场可以为各类用户提供一系列网络化联合应用，包括

支撑国家基础设施安全防护体系建设、自主可控软硬件安全性测试、技术和服务安全性审查和下一代网络与大数据安全研究等应用。

### 4.1.3 网络靶场的特点

网络靶场体系能力是在一体化联合试验体系建设、开展武器装备作战试验需求驱动下提出的新概念，具有仿真性、整体性、动态性、相对性、广泛性、自动化和综合性等特点。

#### 1. 仿真性

网络靶场是指针对真实信息系统的全真模拟环境。建成的网络靶场尽可能贴近实际环境，且仿真过程不超过硬件设备的承载能力，尤其对于重要信息系统和大型关键基础设施的网络系统，网络靶场既模拟了真实的信息系统，又与其相互隔离，不会对其造成任何损害。除了增强的建模仿真工具，网络靶场还提供虚拟敌军对系统进行攻击试验。一个系统进入试验时，一组训练有素的专业人员将通过主动攻击防御系统评估其安全性。网络靶场中还设有虚拟人类行为的功能，这些虚拟人类将通过逼真的日常活动测试网络的安全性和功能，如打开电子邮件、运行应用程序等。

#### 2. 整体性

体系是指能够得到进一步涌现性质的关联或联结的独立系统的集合。网络靶场体系是在一定的战略指导、任务指挥和综合保障条件下，为完成一定的使命任务，通过网络信息系统将网络终端、军事目标和军事系统相互联系和相互作用的各要素、单元、系统，按照一定的组织结构形式而组成的更高层次的整体系统。“整体性”具体表现在：

（1）靶场各要素、单元、系统之间相互关联、相互依存、相互协作、功能互补，形成难以简单划定或区分功能的综合系统，开放性和包容性强。

（2）靶场实质上是一个由人员、技术、装备、场区、法规等要素构成的复杂适应系统，呈现“3+1+1”结构。“3”指实体要素（人、装备、体制编制），“1”分别指渗透性要素（信息）和关系要素（适应性）。

（3）强调发挥靶场指挥信息系统互联、互通、互操作的融合功能，实现靶场各要素、单元和系统的结构演化、一体联动和效能涌现，达到“1+1>2”的整体效果。

#### 3. 动态性

根据系统结构与环境决定系统功能的系统论规律，网络靶场是一个按照相应机理运动发展的整体系统，是“活”的系统，其结构、状态、特性、功能、行为等将随时间的推移而发生变化，这种变化可称之为演化。也就是说，网络靶场具有适应性和进化性，其结构、状态、特性、功能、行为等都处在或快或慢的演化之中。因此，网络靶场体系能力不是静

态的,而是在实施运作中不断发展变化,具有灵活、适变、动态等特性。“动态性”具体表现在:

(1) 靶场任务/运行体系结构能灵活应对不同任务要求,可为创新试验鉴定模式、构置联合试验环境、承担新型试验任务而发生演化,如信息协同能力、任务协同能力、环境效能等。

(2) 靶场系统体系结构在连通性、鲁棒性、脆弱性、抗毁性等方面发生演化,如信息(服务)交互能力、组网通信能力及质量、体系运行的自适应和自协同性能等。

(3) 靶场技术体系结构的演化,表现在指向性、功能性、整体性、规范性、逻辑性等方面。

#### 4. 相对性

网络靶场体系能力是通过使命任务展现的,是其功能和作用与使命任务结合的直接体现,是在某种环境条件和方式手段下“某一任务”“某一时刻”的能力水平。使命任务不同,其能力也不同。“相对性”具体表现在:

(1) 环境条件的相对性。主要指网络靶场遂行使命任务时是否构造实际的战场环境,是否和配装部队的使用结合起来,是否按照实际的任务流程和任务剖面要求来实施运作。

(2) 方式手段的相对性。主要指网络靶场在任务想定拟制、任务条件构造、任务计划制定、任务项目实施中所用方式手段的对比性、创新性和有效性。

(3) 获取数据的相对性。获取与武器相关的资料和数据是网络靶场遂行使命任务时的主要目标,也是网络靶场考核装备作战适用性、作战效能及体系贡献度的前提和基础。受环境条件、数据采集与分析手段的限制,网络靶场任务期间获取的数据具有相对性。

#### 5. 广泛性

当前,网络安全所面临的最大挑战之一就是缺乏在可控环境中进行有效模拟的平台。这种平台要足够大,能够提供真实的模拟环境,同时又要十分灵活,能够制造和模拟出各种可能遭遇的网络攻击场景。网络安全涉及军事、政府、工业等多个领域,包括能源、金融、石油、交通、航空、电信等多个掌握国家命脉的行业。网络靶场需要兼顾不同领域间的差异,尽可能保证整个平台的通用性。网络靶场针对不同的试验目的,可以通过管理控制软件对硬件资源进行调度。

#### 6. 自动化

网络靶场的一个重要特性是自动化。网络基础结构创建后,研究人员可以立即投入试验,可以精确地重复试验条件,并能够反复进行新型研究,可以通过较小的改变实现对测试环境的改变。另外,通过创建一个全自动、互动的处理,来规划、设计、分析并进行测试。用一个大规模的系统配置计划设计靶场,研究人员可以更有效地利用有限的资源,实现更多和更真实的测试。此外,网络靶场必须具备重新配置的快速性,可以模拟网络的多

样性，并在不同加密层级同时处理多个对象。研究人员可以通过简单操作改变试验环境及参数设置。同时，针对真实社会网络威胁的动态性，网络靶场解决了大规模网络测试的时效性和范围不足问题，为试验和分析提供了快速周转时间。

## 7. 综合性

网络靶场涉及多个领域，需要多方合作，可以调动军队、警察、专家、关键基础设施或重要信息系统参与者等多方力量来完成。网络靶场可以建立专门的试验平台对信息系统的安全性进行验证，并与国家安全机构、工业控制部门共享研究数据，整个平台应该具有互联性，方便数据的传输和共享。网络靶场需要耗费巨大的人力、物力、财力，开发周期长，建成周期一般在 4~6 年，长则十几年，投资金额一般为数千万至数亿美元不等。以美国为例，建设国家网络靶场第一阶段就耗时 12 个月，花费了 2500 万美元。

### 4.1.4 网络靶场的任务与目标

#### 1. 主要任务

网络靶场的任务类型主要包括训练、测试与评估和演习 3 类。

在训练任务中，根据靶场用户训练需求，按需构建可反复进行攻防演练的试验运行环境，要充分模拟真实的物理网络（其中的重要环节包括防火墙、路由器、交换机等），操作系统的模拟要多样化，提供的服务要全面，要进行数据采集与处理，评估训练的有效性，有针对性地研究攻击策略及应对办法，同时辅助用户分析如何配置试验环境以获得最佳训练效果。在一步步的研究入侵行为并寻求安全解答的策略中，逐渐提高参训人员的安全意识及网络防范能力。

在测试与评估任务中，网络靶场提供了可重复和可验证的网络测试与评估环境，用于验证信息保障技术、网络防御技术和作战概念。网络靶场测试的对象是信息技术发展的最新成果，其中包括全新的操作系统、系统内核、工作站/终端部件、主机安全系统、局域网安全工具和组件、网络操作系统和设备、网络拓扑结构，以及网络协议等。

在演习任务中，网络靶场支持各种贴近实战的网络想定演习，承包商参与演习规划、想定设计以及具体执行等环节。

#### 2. 建设目标

网络靶场框架将用于构建一致、可重复且可验证的测试与评估场所，用于验证信息保障技术、网络防御技术和作战概念，以达到测试与评估目标。

##### 1) 提高网络空间安全人员的作战能力

网络靶场通过对敌方人员的网络空间攻击效果以及网络防御人员对网络攻击的防护、



监控、监测、分析、诊断与快速响应等防御效果进行评估,以提高网络安全人员的作战能力。以真实的网络作战环境为模拟对象,以各种网络、电子战手段为技术对抗对象,通过模拟真实环境的演练实现网络空间作战实力的大幅提升,在网络战争时期能够确保打赢。网络靶场需提供专业且经验丰富的对抗部队,根据需要执行各种网络攻击想定。通常,攻击行为分为侦察、扫描、访问、权限提升、窃取、攻击、维持和掩藏8个阶段。根据要求,网络攻击想定应涵盖各类攻击行为,包括主动的、被动的、内部和分布式等。

## 2) 验证网络空间防御工具的能力

网络空间防御工具可提供对非授权活动进行防护、监控、检测、分析、诊断和响应等能力。为支撑网络空间防御新兴技术的研究,网络靶场提供一个稳定环境用于网络空间防御新兴技术的设计、实现与验证,其中包括通过对不同安全防御策略的选择与组合验证防御工具的能力。同时,还提供理想的试验环境,用于测试网络空间防御工具和技术的有效性,旨在促进当前技术以及未来新兴技术发展。

## 3) 验证网络空间防御的战术、技术和规程(TTP, Tactics, Techniques and Procedures)

在开发实现网络空间防御技术时,需关注人员、操作及技术在关键基础设施网络安全中所起的作用,标准化TTP将有助于克服安全产品潜在缺陷。标准TTP建立是配置网络安全措施的前提条件,网络靶场将用于验证并提高计算机网络防御的TTP。

## 4) 验证计算机网络安全服务商提供服务的能力

计算机网络安全服务商不同于传统的认证与鉴定,需对服务商可确保的最低服务标准进行评定。网络靶场将用于验证计算机网络安全服务商提供的服务是否达到预定义标准,这些标准涵盖以下5个方面:

(1) 防护:包括脆弱性分析和评估、病毒防护、人员防护与训练和信息保障脆弱性管理等;

(2) 监控、检测、分析和诊断:包括网络安全监控和入侵检测、攻击探测、报警、预测和态势感知;

(3) 响应:包括安全事件上报、恢复和主动反击等;

(4) 维持:包括计算机网络防御条令与规程,计算机网络防御技术的开发、实现与评估,用户认证和安全管理等;

(5) 验证信息保障风险降低策略:信息保障风险的降低涉及风险降低策略的排序、评估和实现。考虑到完全消除风险不切实际,因此,网络靶场可用于验证将风险降低到一定范围内的最优控制方法。

## 5) 提供测试、复制和仿真的能力

网络靶场还应具备以下能力:支持成千上万的虚拟和实际测试节点,并能提供自动测试的能力;根据测试单位的需要和资源的可行性,测试个人计算机安全和大规模网络安全的能力;真实复制相关用户行为及弱点的能力;高度仿真攻防对抗的能力;加速或减缓相

关测试时间的能力；通过集成、复制或模拟技术，测试主机系统安全、网络安全工具和套件的能力；封闭或隔离测试数据的能力；开发与部署创新性网络测试的能力。

#### 4.1.5 网络靶场的功能需求分析

网络靶场应该主要满足的功能需求：

##### 1) 网络空间复杂性安全试验环境需求

进行网络空间复杂性安全试验需要网络靶场具备四方面的能力：一是大规模复杂异构网络的快速复现能力，可复现军用网络、政府网络、金融系统、电信网和物联网等各类复杂异构网络；重现商用无线网络、战术无线网络及控制系统的能力；复制当前及未来作战中复杂的、大规模的异构网络与用户；在相同基础架构上进行多项独立的同步实验。二是复杂用户行为及网络舆情复现能力，可逼真模拟社会网络中人的行为和舆情行为。三是网络空间复杂特征的复现能力，可复现网络空间融合性、隐蔽性、复杂性、无界性、高速性和层次性等复杂特征。四是大规模网络快速灵活重组能力，可从一个试验网络结构快速灵活重组成另一个试验网络结构。

##### 2) 成体系的测试评估与验证能力需求

为了精确测试评估目标系统网络空间安全性、可恢复性和灵活性，操作系统、网络协议、内核等关键软硬件的安全性，网络靶场需具备成体系的测试评估能力。根据当前和未来环境的真实条件，通过完备的测试评估资源库（测试工具库、测试用例库等）及先进的测试评估手段，开展渗透测试、风险评估，对目标系统安全性进行全方位、体系化、自动化测试评估，对各种信息安全保障工具和手段进行定性及定量评估。还要进行网络攻防武器评测验证：新型网络攻防武器研制出来之后，需要对其进行测试验证，是否能有效攻破敌方防护系统，以及是否能有效保护己方目标系统。科学试验和新技术验证：网络空间科研人员研制出新的网络协议、新型网络设备、新的革新成果以及不同网络新技术，在互联网上功能和性能如何，也需要进行验证。在一个网络架构上同时进行多个独立的测试，进而对网络空间研究进行高可信度仿真，同时开发最新的网络测试技术。

##### 3) 高安全隔离与高数据安全的联合试验环境需求

为了并行开展不同安全等级网络的试验而不影响各试验网络与数据安全，需要构建高安全隔离与高数据安全的联合试验环境，提供创新的实地模拟环境。在联合试验环境中可并行开展多个不同安全等级的安全技术测试、各种恶意软件和恶意代码测试等试验，使用或测试新的未经证实的概念或能力，用于保护重要信息系统和关键基础设施，而不用担心试验基础设施安全。并行试验之间不会相互干扰，重要数据也不会试验中泄露。

#### 4) 资源自动配置与快速释放能力需求

为实现网络靶场内部各类异构公用资源（网络、计算、存储、信息等）的集中管控和灵活调用，使其利用率最大化并保证用户对资源使用的有效性，需具备资源自动配置与快速释放能力。

#### 5) 面向服务的公共服务能力需求

为了实现不同网络空间安全试验资源的即插即用、动态共享、重用和互操作，网络靶场需具备面向服务的公共服务能力，建立服务化、智能化、网络化、模块化的网络公用基础设施集成环境，为各功能系统面向服务的部署、集成、运行与管控提供全过程支撑。

### 4.1.6 网络靶场国内外研究现状

世界各国均将网络靶场建设作为支撑网络空间安全技术演示验证、网络武器装备研制试验、攻防对抗训练演练和网络风险评估分析的重要场所。美国政府率先开始了网络靶场的设计与运营。不但建立了多个小型网络靶场，而且还设计建立了国家网络靶场。英国也不甘落后，不仅建设了先进的“国家网络靶场”，还将部分靶场与美国“国家网络靶场”联网，建立了联合网络靶场。此外，日本、加拿大、澳大利亚、以色列和北约等相继建立了自己的网络靶场，欧洲防务署也专门批准了网络攻防测试靶场的建设计划。

可以将网络靶场的发展分为功能探索期、虚拟化模拟期、应用扩展期三个阶段。在功能探索期，针对网络靶场的最初研究是以军事应用为目的的网络模拟，开始于1983年美国国防高级研究计划局（DARPA, Defense Advanced Research Projects Agency）项目和陆军共同投资的SIMNET（Simulator Networking）项目。21世纪初期，主要目的是应对单独的木马类攻击武器，瞄准敌方的靶标软硬件平台，尽量使靶标软硬件平台建立得完美逼真，使之能够测试己方新研制的网络攻击武器是否能够不被敌方的防护软件所发现。这类网络靶场主要有木马测试系统、蜜罐系统等。虚拟化模拟期被称为小型虚拟化互联网靶场时期。此阶段从2005年开始，其目的是提供虚拟环境来模拟真实的互联网攻防作战，一般模拟的网络规模都比较小。采用的技术主要有软件定义网络、云计算等虚拟技术。在这个时期，网络靶场的主要代表有美军的“联合信息作战靶场”“国家网络靶场（NCR, National Cyber Range）”“国防部网络安全靶场”，英国的“网络安全试验靶场”“SATURN靶场系统”和“商用联合网络空间试验靶场法汉姆（Fareham）”，加拿大的“CASELab靶场系统”和“加拿大国家规模仿真实验室”，日本的“StarBed靶场系统”“星平台”和“新一代网络研究计划”，以及我国台湾的“Testbed测试平台”，等等。应用扩展期是大型虚实结合网络空间靶场时期，这个时期从2014年开始，其目的是网络靶场要支撑泛在网，利用虚实结合的网络空间靶场技术，模拟对工控网的新型网络攻击的突现，如模拟解决像“火焰”“震网”等突发性攻击问题。其典型代表有北大西洋公约组织的支持工控网攻防测试的NATO

网络靶场，欧洲防务署的网络攻防测试靶场等。这些靶场不仅为研究人员提供了云计算、大规模网络安全和保密等领域的核心研究能力，而且为研究人员提供了一系列的分析与仿真工具，使得用户能够在完全可重复的试验条件下对真实世界大规模网络进行行为建模，进而探索这些网络系统所存在的缺陷。

美国在网络靶场建设方面，除众所周知的国家网络靶场（NCR）外，美军还陆续启动了“国防部信息确保靶场”“联合网络空间作战靶场”“海军网络空间作战靶场”“联合信息作战靶场”“战略司令部网络作战靶场”“陆军国民警卫队增强型网络训练模拟器靶场”等多个赛博靶场的建设。目前，这些靶场相继建成并投入使用，在网络技术装备试验和网络作战人员训练等方面发挥着重要作用。此外，还有美国惠普公司、英特尔公司和雅虎公司正在联合开发“全球云计算试验平台”等。

2008年5月，美国DARPA拉开了建设一个从各方面来讲逼真度都非常高的NCR的序幕。经过2009年1月至2012年10月近四年的建设，DARPA于2012年10月将位于洛克希德·马丁公司设施内的NCR移交给了美国国防部试验资源管理中心。目前，NCR已具备了开展试验与训练的能力。据美国国防部称，NCR已被用于对一个模拟了15000个高逼真节点的网络进行了试验。靶场在2012年承担了近10项网络试验任务，并将逐步承担更多的网络试验任务。NCR是美军最大的网络靶场，可以模拟因特网等大型网络，其特色主要体现在以下四个方面：体系结构安全可靠、试验设计简便易行、靶场配置自动高效、复位还原自动进行。最终目的是保护美国的网络安全，防止美国遭受敌人的网络攻击，并能对敌方展开在线攻击。具体包括网络攻防实验床Emulab、DETERlab及PlanetLab。

2010年，英国正式启动了国家级网络实验场。据悉，该实验场整体十分复杂，可高度模拟现今互联网的运作，通过各种设备模拟真实环境，但同时又与互联网相互隔绝，因此英国军方和政府、学术机构可以在安全、可控的实验环境中展开各种演练。这个实验场与美国网络战靶场连接，进行高强度网络空间作战的全球演练。该网络实验场将在研究网络威胁、保护基础设施安全方面发挥重要作用。据报道，该网络实验场由美国军火商诺思罗普·格鲁曼公司搭建，将与诺思罗普·格鲁曼公司在美国马里兰州建立的美军“网络空间解决方案中心”以及全球其他网络实验室互联，以增强网络模拟能力，进行全球范围内的网络攻防试验。“Breaking point”是英国另一个网络靶场系统，由英国Ixia公司开发建立。它能够进行漏洞仿真、目标仿真、流量仿真、逃避仿真、数据丢失预防的相关数据仿真、移动用户群仿真等。

2012年10月，澳大利亚与美国诺思罗普·格鲁曼公司签署了一份合同，为澳大利亚新南威尔士大学、澳大利亚国防学院堪培拉校园建立网络测试靶场。该靶场主要供澳大利亚国防学院为澳大利亚军队训练和培养军官，以及为澳大利亚军事网络技术的发展、测试和评估提供工具和平台。

日本于2002年由情报通信研究机构（NICT）负责研制了“星平台（StarBed）”，StarBed目前有三个版本，其功能扩展到网络安全、服务质量、复杂有线/无线网络、网络安全物理系统的构建、软件实现、真实场景的评估和大规模网络试验环境与仿真。该平台2014年在用的实验组总节点数已经达到1398个，并且其存储容量为60TB。另外，还分别建设了“计算机系统通用平台”和“防卫信息通信平台”。与此同时，日本十分关注与美国共同进

步,引进美国的相关技术来改善本国的不足,持续提高网络靶场的能力。

加拿大也建立了网络试验平台,该平台能提供大规模网络安全和保密、云计算、系统分析和仿真工具,能支持网络系统的行为建模、互联网新技术(武器)的鉴定和评估。

以色列埃尔比特系统公司也推出了网络战训练系统,埃尔比特系统公司与总部设在美国的“断裂点”(Breaking Point)网络安全公司联手开发了一种新的流量发生引擎,这种引擎已被集成到了网络靶场,它可以自动向仿真结构注入攻击。

我国网络靶场建设目前处于起步阶段,中国电子科技集团、中科院计算所、北京邮电大学、国防科技大学、四川大学、CNCERT/CC、中科院信工所、哈尔滨工业大学均建设了自己的网络靶场;信息工程大学和陆军工程大学也正在建设军用网络靶场;合天网安实验室的互联网教学靶场,使用的高校达300余所,使用的学生达3万余人,在举办的XP挑战赛、强网杯挑战赛、暴恐音视频挑战赛等全国性系列网络安全竞赛等比赛中发挥了重要作用。我国目前研究的网络靶场主要用于电子信息对抗、仿真、产品试验及检测、教育和培训等。在理论研究方面,我国学者陈灏根据软件工程的开发模式设计了一款基于KVM技术的网络靶场系统,同时设计内置蜜罐靶场的网络拓扑。黄本雄等人设计了通过蜜罐架构的虚拟靶场环境。从体系应用角度来讲,我国现有的网络试验环境或测试床规模还较小,且主要针对某一专业领域,尚不适用于体系化的网络空间安全科研试验与测试评估。在国家网络靶场建设方面,无论是靶场基础理论研究、关键技术和产品研发,还是网络空间安全风险评估研究,我国与世界强国相比都还存在着不小的差距。

## 4.2 网络靶场的设计与规划

从网络系统自身安全要素出发,实体、平台、通信、数据、管理安全是网络靶场的五个安全要素。这五个要素能提供合理设置的硬件环境;能设定相应的版本和补丁可控的操作系统以及各个系统平台漏洞;网络上能提供各种服务应用软件、加密和未加密的通信协议、各种级别的数据访问权限控制;允许/禁止网段内数据包过滤和嗅探;允许一定程度段内信息欺骗(中间人攻击)、人为的管理漏洞(弱口令、口令重用、敏感文件无规范放置等)和详尽的机器状态日志。

### 4.2.1 网络靶场的设计要素与架构

#### 1. 设计要素

网络靶场设计要注意考虑以下问题:

- (1) 尽可能重现真实网络物理状况,包括路由器、交换机、服务器、防火墙、入侵检

测（防御）设备、无线接入设备等要素。

（2）尽可能全面反映各种平台，各种服务工作情况。

（3）尽可能模拟具备不同安全意识等级的网管人员的管理策略和方法。

（4）尽可能提供全面记录各种入侵的日志，提供数据融合功能，把攻击日志与被攻击日志原始数据融合生成报表，便于学习提高。

## 2. 系统设计

网络靶场是建立在统一基础设施上的可重用试验平台，其系统架构自底向上可分为基础设施层、服务支撑层和试验表示层 3 层结构。网络靶场系统架构如图 4-2 所示。

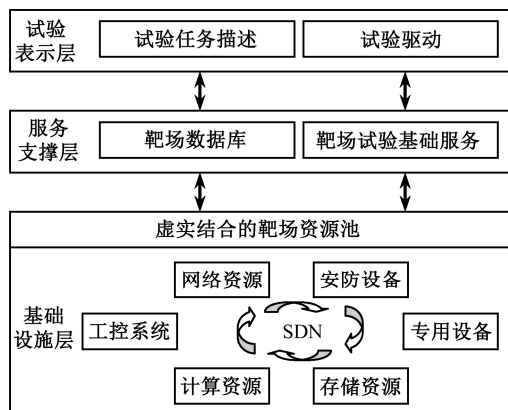


图 4-2 网络靶场系统架构

基础设施层包括计算资源、存储资源、网络资源和安防设备等基础设施，为网络靶场提供基本的系统资源。通过云计算技术将各类资源虚拟化为靶场资源池，并通过软件定义网络（SDN，Software Defined Network）技术集成各类虚拟资源以及工控系统、专用设备和无线设备等实物资源，该层通过一组资源管理工具对虚拟和实物资源的运行状态进行监控和管理，形成可根据网络靶场试验需求弹性扩展的资源集合。

服务支撑层由靶场数据库和靶场试验基础服务组成。靶场数据库包括测试工具库、攻防工具库、日志数据库、资源镜像库、试验想定库和靶场配置库等；靶场试验基础服务包括消息、系统状态、数据采集、预警、日志和安全等服务。服务支撑层基于靶场数据库资源，通过服务化和消息化形式提供网络靶场的管理、调度、运行和监控等功能。

试验表示层提供靶场试验任务描述和试验驱动功能，包含试验配置、试验控制、流量产生、用户接口和试验评估等功能模块。试验表示层通过规范化语义试验描述语言描述了靶场试验的配置、部署、控制和输出等特性，对靶场试验过程在统一视图下进行描述，将网络靶场试验需求和部署方式转换成系统操作指令，下发至服务支撑层执行。

### 3. 网络靶场的实施

建设符合上述标准和要求的靶场后,网络战人员可以方便地在这个环境中,反复演练入侵手段和策略,测试发现未发布的新漏洞,试验改进新工具,同时也在入侵侦察中相应提高自身的网络安全的防御意识和能力。

图4-3是一个网络靶场系统的实施结构图。其实施思想是:首先,训练人员在攻击端从工具服务端获得相应的攻击工具或攻击方法,开始对目标机器进行攻击;同时攻击行为记录模块开始对攻击行为进行记录;然后,行为检测模块检测到攻击行为;脆弱性模块开始接受攻击行为的压力测试,达到不同程度的被入侵效果;通过行为控制模块可以调节攻击行为允许的限度,起到了调节攻击难度的作用;被攻击效果记录模块对攻击行为进行详细记录,收集原始数据,并在不同层次上进行行为跟踪;最后,攻击端的行为记录和被攻击端的被攻击效果记录被数据融合和系统融合,得到详细的攻防效果分析报告,作为攻击后的经验总结和教学使用。

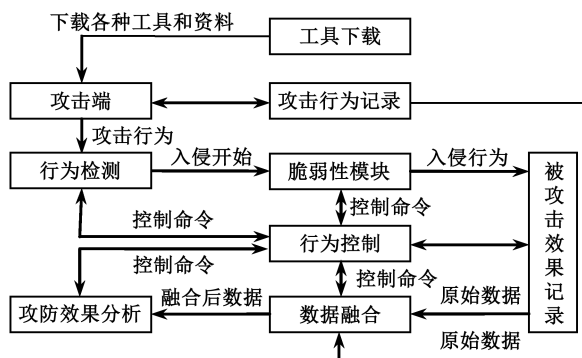


图 4-3 网络靶场系统的实施结构图

## 4.2.2 网络靶场的系统实现

### 1. 物理组成

网络靶场试验环境在物理上由计算资源服务器、存储设备和网络仿真服务器等设备通过高性能、可编程的网络设备互联,基于 SDN 技术实现各类资源的互联互通、端口映射和流量重定向。系统物理网络环境分为管理网和业务网两类,分别实现环境配置、部署、指令传输和目标系统组网功能,管理网和业务网之间相互隔离,通过 SDN 控制器进行控制指令层次的互操作,业务网在防火墙保护下对外提供试验接入服务。网络靶场试验环境物理架构如图4-4所示。

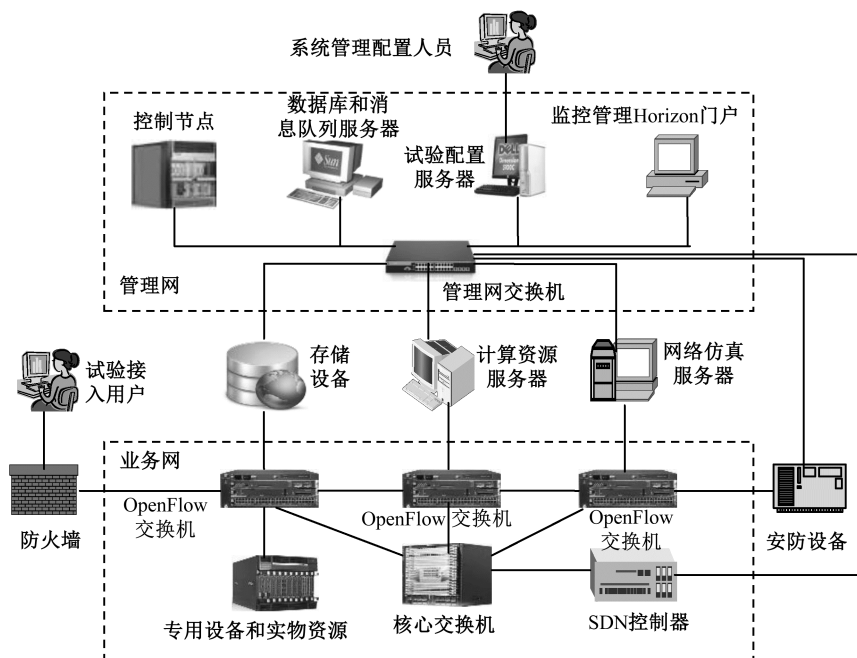


图 4-4 网络靶场试验环境物理架构

## 2. 逻辑组成

网络靶场试验环境在逻辑上是一个服务化资源管理框架，平台通过维护虚拟化资源池中的资源向上层试验提供服务。靶场逻辑组成可在 OpenStack 通用资源管理框架上扩展。OpenStack 是一个可灵活扩展的云计算基础设施即服务（IaaS，Infrastructure as a Service）资源管理框架，包括计算管理、镜像管理、对象存储、网络管理、块存储、认证管理和界面展示等子系统，所有子系统和服务集成起来提供 IaaS 服务，子系统和服之间通过标准化 API 实现集成和相互调用。

网络靶场试验环境逻辑架构如图 4-5 所示。靶场物理基础设施通过一组高性能服务器集群、高速组网设备和海量存储设备为上层系统提供计算、存储和网络等基本系统资源，经由虚拟化资源抽象层转化为虚拟化资源池，通过 API 对外提供服务。首先，用户通过规范化的试验描述语言完成特定靶场试验任务的形式化描述。资源申请组件根据靶场试验任务描述从资源池中选取所需的资源。对于新增资源，用户可利用资源注册模块注册并扩展到资源池中。其次，配置生成组件根据试验描述对所选取的资源进行配置，形成配置文件并下发到环境构建层执行。在环境构建层，网络靶场通过一组 API 访问虚拟化资源池中的资源，基于网络构建、计算构建、镜像管理和存储管理等功能模块，生成满足靶场试验需求的资源组合，并通过核心服务加载组件加载试验所需平台软件和核心服务，形成一个可运行靶场试验实例。用户可使用运行管控组件实现试验初始化、试验开始和试验终止等功能。在试验过程中若需调整系统参数和资源配置，可将更新需求输入动态重构组件，系统调用重构 API 进行资源重构操作。系统评估组件监控系统中资源运行状况，记录日志信息，



进行性能评估和负载均衡。

网络环境是网络靶场的核心组成部分，因此网络资源构建模块包含 OpenStack 网络组件 Quantum 和基于操作系统容器的虚拟化网络仿真组件，共同实现网络化信息系统中大规模 IP 网络的按需配置、部署和接入，网络构建模块逻辑架构如图 4-6 所示。其中虚拟化网络仿真组件包括网络模拟和虚拟组网设备。系统根据配置文件解析网络构建需求，将网络拓扑特征和链路参数（带宽、时延和抖动等）通过消息中间件传递给网络仿真组件，网络仿真组件根据消息内容构建所需虚拟网络设备和虚拟链路；网络接入参数〔IP 地址、网桥接口和虚拟局域网（VLAN，Virtual Local Area Network）等〕则由消息中间件传递给 Quantum 组件，实现虚拟机接入控制。

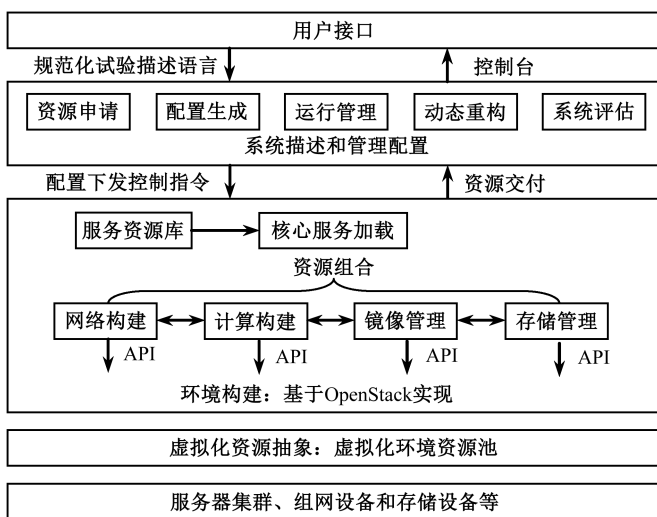


图 4-5 网络靶场试验环境逻辑架构

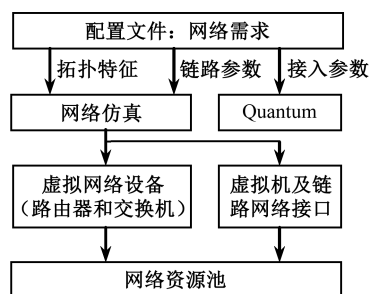


图 4-6 网络构建模块逻辑架构

### 3. 运行架构

靶场试验环境构建过程将不同类型的资源根据试验需求和相互依赖关系进行动态组合、协同和互操作。网络靶场试验运行时，将系统运行所需各类资源统一注册，再通过可灵活配置的网络进行关联和集成，实现资源的按需调度、配置和互操作，为用户提供一种与真实环境无差异的系统运行环境，支撑系统研发和测试等。网络靶场试验环境运行架构如图 4-7 所示。

网络靶场试验涉及资源数量多且类型复杂，为提高硬件资源利用率和仿真试验环境构建效率，需将目标资源调度并映射到合适的物理资源上。OpenStack 网络组件中的 ChanceScheduler 和 SimpleScheduler 等调度算法难以实现服务器动态负载均衡，不适应网络化信息系统调度运行场景。因此，在目标环境部署时，网络靶场试验环境构建系统根据性能评估组件通过资源状态感知和最优映射策略进行资源调度和部署。

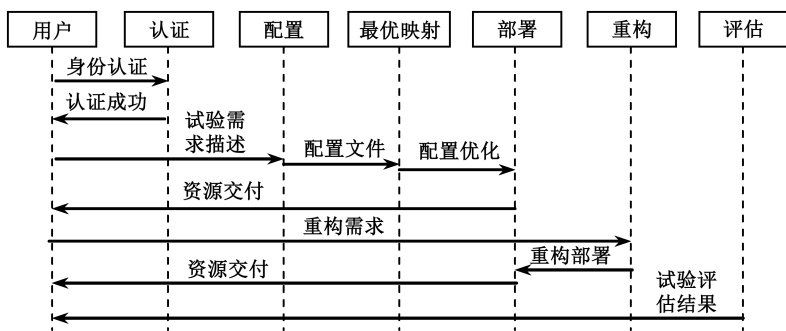


图 4-7 网络靶场试验环境运行架构

### 4.2.3 国家网络靶场系统设计架构及与传统靶场的比较

靶场体系架构的建立有助于从系统层面思考问题，关注纵向、横向，实现大系统的互联、互通、互操作，用一体化思想统筹建设项目，既考虑已有信息系统资源，又分析未来系统建设，为靶场综合集成奠定基础。

国家网络靶场体系结构设想如图 4-8 所示，主要包括靶场基础环境（基础层）、数据资源库（支撑层）、服务支撑（支撑层）、靶场应用（功能层）、标准规范体系和安全保障体系。

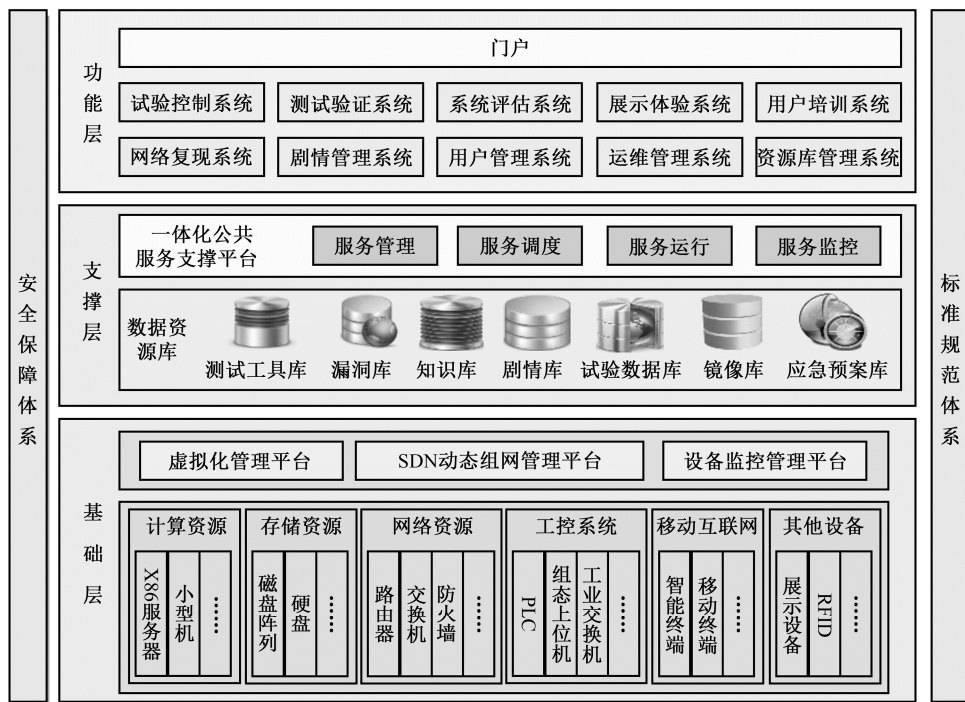


图 4-8 国家网络靶场体系架构设想

其中,靶场基础环境是网络靶场运行的基础,支撑靶场功能系统的运行,具体包括运行资源建设(包括计算资源、存储资源、网络资源)、目标系统建设(工控系统、移动互联网等)、虚拟化管理平台、SDN 动态组网管理平台和设备监控管理平台等。虚拟化管理平台、SDN 动态组网管理平台、设备监控管理平台对靶场的物理资源和虚拟资源统一管理和调度。其中,工控系统包括可编程逻辑控制器(PLC, Programmable Logic Controller)、组态上位机和工业交换机等;其他设备主要是展示设备和射频识别(RFID, Radio Frequency Identifier)设备等。虚拟化管理平台通过对靶场中各类虚拟资源(如计算、存储、网络等资源)的统一调度和管理,从而提供可根据试验需求弹性扩展的节点虚拟机资源;SDN 动态组网管理平台对所有虚拟网络进行集中式监、管、控;设备监控管理平台主要对靶场中各类硬件设备(如服务器、交换机、安全设备、工控设备等)的运行状态进行实时监控和管理。

数据资源库是靶场的核心资源,是靶场运行和试验操作的工具、数据和知识保障,支持靶场业务的开展和试验的运行。数据资源库分为三大类,分别是核心基础资源、试验支持资源和服务支撑资源。核心基础资源包括测试工具库、漏洞库、镜像库,以及防御产品库和软件库等。试验支持资源包括剧情库、试验数据库、知识库,以及模型库等。服务支撑资源包括应急预案库,以及情报库等。

一体化公共服务支撑平台采用面向服务的架构(SOA, Service Oriented Architecture)的思想进行搭建,实现服务管理、服务调度、服务运行和服务监控等各个层面的解耦,达到完全的消息化、服务化,以及业务的无关性;为各类用户提供信息共享与协同、信息聚合、服务聚合,以及能力聚合等面向服务的典型应用支撑能力。

靶场功能层提供靶场试验的管理和应用业务,分为网络复现、剧情管理、试验控制、系统评估和展示体验等十个功能系统,通过统一门户与用户进行交互。

安全保障体系从物理环境安全、安全基础设施、网络安全、计算环境安全、应用安全、安全管理、风险评估等七个方面采用技术手段和措施,确保靶场可靠稳定运行和试验安全可信开展。同时,采用试验隔离和数据擦除等技术手段,确保靶场中同时开展的试验相互独立,靶场中的敏感信息彻底销毁,无泄露风险。

标准规范体系是保证靶场高效运行和协同的重要保障,网络测试语言、测试过程、资产、数据库和试验过程的规范化、标准化将贯穿于一个完整的网络试验生命周期中。

国家网络靶场与传统靶场的比较见表4-1所示。

表4-1 国家网络靶场与传统靶场比较

属 性	传 统 靶 场	国家网络靶场
安全性	安全级别单一	根据任务类别设置相应的安全级别,对测试资源进行消毒,安全、可测量的网络实验环境
硬件配置	手动配置测试设备和测试硬件脚本	动态安全地配置几千种异构资源以满足并行测试任务要求
软件配置	手动配置和管理测试软件脚本	图形用户界面用于配置测试环境,高级语言用于测试管理和资源分配

续表

属 性	传 统 靶 场	国家网络靶场
可用性	用户需要携带一切必需资源 基于有限技术进行作战实验，没有更多选择	自动加载技术和配置条件 具备协助实验进行的软件库 提供科学评估及网络攻击、网络防御等想定服务
仿真置信度	仿真与现实存在偏差 有限的无线和移动自组网能力	物理、虚拟和仿真之间大规模组合 可对商用或军用的无线/控制系统进行仿真 可扩展的开放式体系结构 芯片级的异构虚拟机 可整合使用或更换 TCP/IP 协议栈
测试时间	受限于现实时间，无法更改测试速度	可提高测试速度用以更快获得测试结果 可降低测试速度用以分析，以便进行优化
测量科学性	只能收集原始数据	定性/定量评估网络安全技术 精确的数据收集、分析和显示 不同设备之间高度同步
业务生成机制	自动生成	真实模拟人类的行为和弱点来进行业务生成

#### 4.2.4 网络靶场核心技术

在网络靶场的建设过程中，将对靶场建设和运行过程中涉及的网络复现、多维度测试、靶场资源动态管理等一系列关键支撑技术进行研究和突破，具体包括：复杂异构网络快速复现及重构技术、网络空间安全自动化多维度测试技术、面向任务的靶场引擎构建技术、靶场资源自动配置与快速释放技术、非易失性存储数据安全擦除技术、靶场安全隔离与受控交换技术、特种木马及高级持续性威胁（APT，Advanced Persistent Threat）攻击行为识别技术、网络追踪技术等。

##### 1. 复杂异构网络快速复现及重构技术

复现目标类型复杂、异构多样，为实现快速复现，节约复现成本和代价，避免“烟囱式”的目标复现，要求平台满足灵活重组、快速重构的要求。基于 SDN 动态组网技术和虚拟化技术，在统一共享的物理网络设施上，开展大规模复杂网络快速可复现及重构技术的研究。

##### 2. 网络空间安全自动化多维度测试技术

根据用户的测试需求，将人工智能、决策论等相关理论方法和技术手段引入平台的测试评估过程，构建科学合理的测试评估模型，自动化调用平台的计算、存储资源和漏洞库、知识库等资源，以及各类测试工具，自动从效果、效率、成本、难易程度等多个维度综合衡量，实现对设备级、分系统级、系统级、体系级的网络空间安全性试验验证，提高测试

评估的客观性、准确性与效率。

### 3. 面向任务的靶场引擎构建技术

基于“面向服务”和“软件定义”的思想，研究基于 SDN 的网络基础设施构建、基于面向服务架构的服务化集成平台构建，以及基于虚拟化的靶场资源快速构建等技术；建立具备面向服务、动态重组、按需分发等能力的高动态、可重构基础网络环境，能够根据各类作战任务需要，快速构建国家网络靶场试验测试软硬件条件，实现网络资源按需分配、全网策略智能决策、身份认证与鉴权的统一管理，满足试验任务需要。

### 4. 靶场资源自动配置与快速释放技术

靶场的网络平台可为用户提供丰富的海量异构资源（网络、计算、存储、信息等），需要实现对这些公用资源的集中管控和灵活调用，使其利用率最大化并保证用户对资源使用的有效性。通过对异构资源进行抽象描述并进行统一标志，形成资源目录，同时建立靶场资源管理平台，实现对靶场资源的发现与自动推送、实时监视、动态调度、智能控制以及快速释放。

### 5. 非易失性存储数据安全擦除技术

研究专门针对试验中非易失性存储数据安全擦除技术，对靶场试验中产生的过程数据进行保密性保障以及实时删除，对非易失性数据进行快速安全擦除以及自毁。在试验结束后可以自动擦除数据、拆除测试平台、回收所用资源，防止试验参数和信息外泄，形成封闭与隔离测试的安全能力。

### 6. 靶场安全隔离与受控交换技术

靶场安全隔离与受控技术包括数据隔离摆渡、多核并行摆渡处理及安全隧道加速技术，通过应用交换、审计监察、安全隧道、身份认证、格式检查、协议重组和交换代理等功能满足两网间在配置指令下发、状态数据上报等过程中的安全需求，为靶场功能系统与各个试验的交互过程提供可靠安全保障。

### 7. 特种木马及 APT 攻击行为识别技术

从分析特种木马在植入、潜伏、活跃各个阶段的不同特征，0Day 漏洞（未公开没有补丁的漏洞）、软件通用漏洞特点，APT 攻击经常采用的弱口令猜解尝试、文件类型伪装欺骗、ARP 欺骗、DNS 劫持和共享带威胁的文件等几种典型的攻击行为入手，突破木马行为辨析与漏洞分析技术，旨在发现、识别、测量、跟踪可确定特种木马、软件漏洞和典型攻击行为的发展过程，通过关联分析实现对特种木马和 APT 典型入侵行为的识别，评估其破坏程度。

## 8. 网络追踪技术

网络追踪技术将加强蜜罐、蜜网等网络诱骗技术的研究,深入分析各类攻击行为特征,深入了解网络攻击手段、攻击方法和攻击目标等,为攻击追踪和调查取证提供依据,实现网络攻击行为的快速跟踪溯源、精确定位。

## 9. 大规模网络仿真环境构建技术

对于国家靶场来说,需要能够重现出大规模的军事、政府和商业网络,由于网络的规模庞大、覆盖范围广,形态多样而且动态变化,靶场难以利用有限的物理资源真实重现各类网络。故需要采用仿真的方法以扩大靶场的规模,且尽可能减少与真实网络环境的差异性,同时根据不同的试验要求和对象按需部署,以满足靶场试验环境在结构、规模和节点要素等方面的要求。

## 10. 靶场试验时钟同步技术

在进行试验时,为提高试验的逼真度,通常需要将外部的实际设备与系统作为配试系统接入靶场。由于这些真实资源与靶场中的虚拟资源在时钟同步方式、描述精度与运行方式等方面存在差异,而且在大规模网络环境中存在不可预知的网络延时,故需要解决真实资源与虚拟资源之间的精准时钟同步问题。

## 11. 靶场试验运行控制技术

网络靶场试验运行控制技术主要包括试验的进程控制和调试控制技术。其中,试验进程控制技术主要包括进程的开始、跳转、加减速、冻结、恢复和结束等,试验过程的缩短与延长是通过运行不同粒度的时间驱动来实现的。试验调试控制技术主要通过调整试验设定中的事件顺序来完成的。

### 4.2.5 网络靶场能力体系

根据研究的视角不同,网络靶场体系能力的总体构成也会有不同的表述。着眼信息系统的主导地位和网络靶场的组织功能,可将网络靶场体系能力分为7个部分,如图4-9所示。

#### 1. 信息支撑能力

信息支撑能力,是指利用网络靶场指挥信息系统和其他信息设备,为网络靶场高效运行提供保障的能力。具体包括信息生成能力、信息获取能力、信息处理能力、信息存储能力、信息传输能力、信息分发管理能力和信息安全保密能力。信息支撑能力是靶场信息资

源渗透到各种能力中的基础性功能和支撑条件。信息资源是靶场最大、最宝贵的资源。开发和利用好信息资源，既是网络靶场要素能力和任务能力实现功能耦合、结构演化和效能体现的有力保证，也是推进网络靶场体系能力建设意义所在。

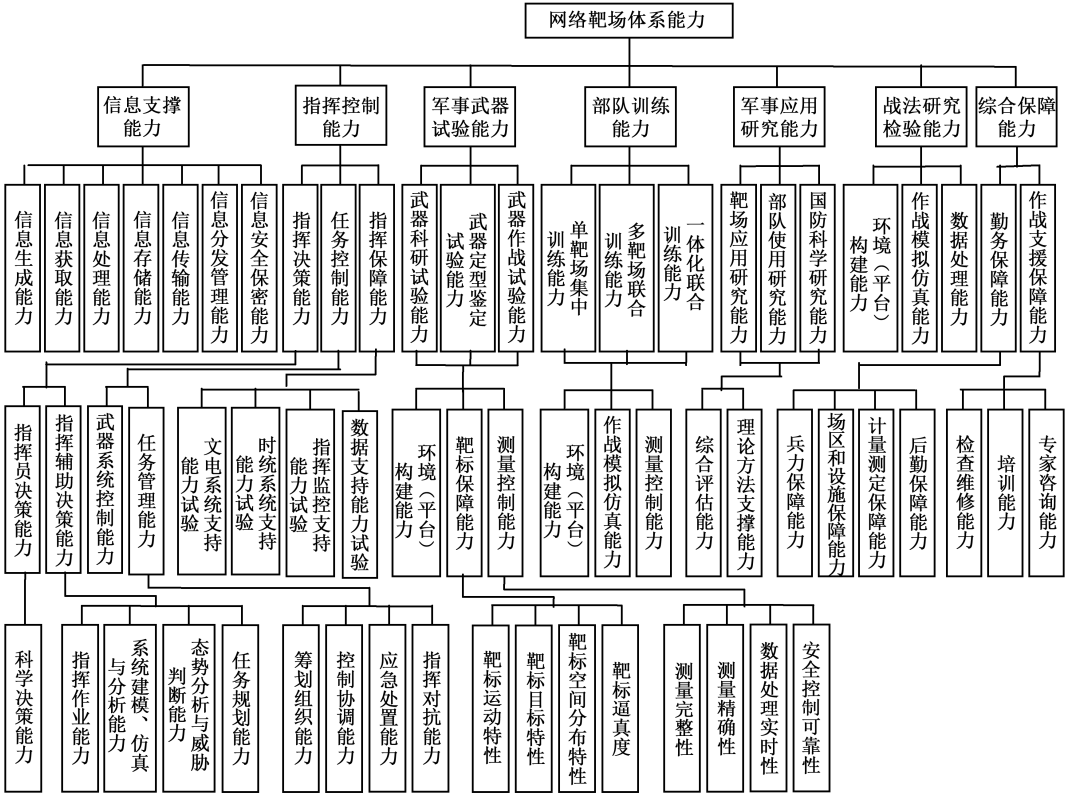


图 4-9 网络靶场体系能力总体构成

2. 指挥控制能力

指挥控制系统包括各级指挥所、指挥中心和指挥单元，它是网络靶场的“大脑”和“神经中枢”，主要功能是信息监控、辅助决策、任务管理、文电系统处理及数据支持，实现不间断、无缝隙的指挥等。指挥控制能力，则是指指挥员及其指挥机关运用靶场指挥信息系统对靶场各力量及其行动任务进行运筹决策和控制协调的能力，具体包括指挥决策能力、任务控制能力和指挥保障能力。

3. 军事武器试验能力

试验能力是军事靶场首要的基本功能。武器试验按照试验性质或目的主要分为武器科研试验、武器定型（鉴定）试验、武器作战试验。军事武器试验能力的指标主要包括环境（平台）构建能力、靶标保障能力、测量控制能力等因素。其中，靶标保障能力主要考核靶标的运动特性、目标特性、空间分布特性和逼真度等因素；测量控制能力主要考核测量

完整性、测量精确性、数据处理实时性和安全控制可靠性等因素。

#### 4. 部队训练能力

训练能力也是网络靶场的基本功能。网络靶场应充分利用靶场人员、技术、装备和场区资源，为部队实战化训练提供对抗环境、作战对手和战术战法，成为部队体系作战能力的“检验场”或“练兵场”。部队训练能力的指标主要包括环境（平台）构建能力、作战模拟仿真能力、测量控制能力等因素。

#### 5. 军事应用研究能力

网络靶场具有人员、技术、装备、设施和环境条件，是开展军事应用研究活动的理想场所。军事应用研究功能包括靶场应用研究、部队使用研究和国防科学研究等。军事应用研究能力重点考核网络靶场的理论方法支撑能力和综合评估能力。理论方法主要包括武器试验方法、作战训练方法、测量方法、数据处理方法、评估方法等。

#### 6. 战法研究检验能力

战法研究检验能力和作战支援保障能力是目前网络靶场需要发展的辅助能力。战法研究检验能力的指标主要包括环境（平台）构建能力、作战模拟仿真能力、数据处理能力等因素。

#### 7. 综合保障能力

综合保障能力主要指为网络靶场运作提供勤务保障和作战支援保障的能力。其中，勤务保障能力主要考核兵力保障能力、场区和设施保障能力、计量检定保障能力和后勤保障能力等因素；作战支援保障能力主要包括检测维修能力、培训能力、专家咨询能力等。

### 4.3 美国国家网络靶场的规划与建设

美国国家网络靶场项目是美国为巩固国家网络空间安全，实现打赢网络空间战争的一项重大举措。为了提供网络武器装备的试验和评估能力，2008年年底开始，美国 DARPA 牵头，60 多家企业与研究院所参加，计划用 6~7 年，分四个阶段建成实用的国家网络靶场。2012 年该项目已经完成第二阶段的建设任务。据报道，2012 年 10 月 1 日，美国国防部试验资源管理中心已经正式从 DARPA 接管国家网络靶场，标志着其已从实验室演示阶段进入全面部署应用阶段。通过着力发展网络靶场，可支撑网络作战研究和网络武器装备验证，提升评估能力，为国家网络战略决策奠定基础。



### 4.3.1 远景、目标和功能

#### 1. 远景

按照美军的构想,美国国家网络靶场将成为进行先进网络研究和测试的独立设施,可以在单一基础设施上同时进行多个独立的、多重安全级别的实验和测试,为特定试验分配具体的资源,并搭建临时的逻辑试验平台,同时简化靶场范围内新代码的引入和测试程序。通过该靶场,人们可对大型网络或全球信息栅格(GIG)进行高置信度仿真,并复现各种复杂、异构的大规模网络,在典型的网络环境中对各种攻防手段、信息保障工具和软硬件工具进行定性及定量的评估,以此开发出最新的网络测试技术。支持多个并行或分段试验,试验结束时,靶场将释放分配的试验资源,由靶场完成回收。通过使用硬件和软件自动化工具,可以快速配置网络参数并模拟复杂的大规模异构网络,模拟网络的多样性,同时灵活地处理不同类型、不同层次的多个任务。能够提供新的开发服务,寻求一种提供在安全和现实的环境中测试真实网络作战能力的方法,并对云计算和存储架构提供安全保护。靶场能够演示和研究目前最具破坏性的网络病毒以及隐蔽性最强的恶意代码,同时将其传播有效控制靶场范围内,避免向公用或军用网络泄露。此外,国家网络靶场还将有能力测试和评估更复杂的网络攻防技术,包括恶意软件、木马程序、分布式拒绝服务攻击、主被动防御手段等。在植入计算机病毒和恶意代码的同时,能够隔离测试平台,阻断其向外部网络感染的路径,即保证靶场是一个完全封闭的“隔离防疫区”,确保其不同安全性和灵敏度水平下同时进行多项测试。使网络空间作战官兵能够了解网络空间行为的影响和潜在的防御手段,同时方便技术人员在测试完成后快速清理查杀并重新配置参数。

美国国家网络靶场的主要特点有三个方面:

(1) 任务领域方面:在进行国家网络靶场的体系建设与顶层设计时,进一步完成网络空间人才教育培养、产品研发试验、产品安全性论证与测试、技术演示验证、安全体系规划能力测试与评估等任务。

(2) 行业领域方面:国家网络靶场涵盖政府、国防、金融、电信和工业等领域。

(3) 应用领域方面:提供一系列网络化联合应用,如国家网络基础设施安全防护体系建设、技术和服务方面的安全性审查、下一代网络与大数据安全研究和自主可控软硬件安全性测试等。

#### 2. 目标

上述远景要成为现实,国家网络靶场项目要达到以下目标:

- (1) 对大规模军用和政府网络具有复用的能力;
- (2) 对商用和战术无线网络及其控制系统具有复用的能力;
- (3) 能够使用某种特定功能、效果或设施,连接分布式网络,制定设施及资源方案;
- (4) 能够利用交互性测试组件进行设计、配置、分析、监控和释放试验资源;
- (5) 靶场管理软件具有鲁棒性;

- (6) 大型异构系统或节点池具备快速集成新节点的能力;
- (7) 新机器副本能够快速生成并进行系统集成;
- (8) 具有新型网络协议集成的能力;
- (9) 重新使用测试工具包/仓库, 用于方案配置与系统架构的建立;
- (10) 数据采集、呈现和分析做到量化;
- (11) 人类行为和弱点能够真实地重现;
- (12) 能够逼真地模仿复杂的国家级网络攻防;
- (13) 能够支持专门现场的安装、故障检测和测试;
- (14) 能够有效地控制测试时间;
- (15) 能够对测试、数据库和网络进行封装和隔离;
- (16) 经验数据库和测试样品能有效地保存, 以供后来需要时使用;
- (17) 建有恶意软件数据库。

为实现上述目标, 国家网络靶场所提供资源的最低标准如下:

(1) 所必需的人员。必须有设计、操作与维护靶场的相关人员参加, 还应包括或部分包括工程师、系统管理人员、靶场管理人员、测试管理人员。

(2) 所必须具有的管理职能。包括安全管理、资格认证、测试计划和测试过程的管理、操作规定和管理、复制大规模网络和子网的管理能力。

(3) 有效复制军民无线网络及其控制系统的能力。

(4) 具有兼容指定任务功能及满足基本条件的能力, 能自动连接分布式、自定义设备。

(5) 具有监测、设计、分析、配置以及释放测试资源的一整套测试和兼容设备仪器。

(6) 成熟稳健的靶场管理套件。

(7) 在大规模异构系统(节点)中, 可快速部署、新添节点, 并进行系统集成。

(8) 具有快速生成、集成和复制新设备的能力。

(9) 对最新标准与协议能实时快速地集成。

(10) 应配有测试工具箱和知识库, 拿出可重用配置方案并建立基本架构。

(11) 数据采集要高质量, 并能进行分析与演示。

(12) 人类网络行为及优缺点能够真实地复制和再现。

(13) 国家级高质量攻防对抗要有能担当、能胜任的高级别力量参与。

(14) 要有网络作战的场所, 能有专门人员提供有效的现场安装、故障排除与测试。

(15) 能动态地掌握相关测试时间。

(16) 能在封闭与隔离的环境下进行测试、数据存储和网络运行。

(17) 要有用于知识管理的存储测试方案和案例, 并建立知识仓库使经验不断累积。

(18) 要开发大量的攻防软件工具。

### 3. 功能

该靶场的第一个功能是自动化。图形用户接口有一个拖放功能可加快网络基础结构的构建, 该结构创建后, 可立即投入试验, 以便节省试验时间。通过该接口可方便地设定主

机、环境参数、敌人类型和系统延迟。

第二个功能是可人为地设置被测系统出现故障，然后重启再试。该靶场能利用保密和非保密网络及软件进行试验。通过自动设置，可快速操纵很多场景并开发出新结构。

第三个功能是网络态势感知。在国家网络靶场中可以让用户改变传感器在网络中的位置，对各种态势感知工具进行测试，以便比较它们的性能。

第四个功能是动态地调整网络作战试验和仿真的速度。当在观察系统的启动过程和操作过程时减慢网络安全试验速度；当在测试网络带宽时，可以正常速度或加快速度运行。

第五个功能是高逼真的实时仿真和虚拟试验。能够对武器系统、交战中大规模异构复杂网络 and 用户等进行形象直观的仿真模拟；与虚拟敌军展开交互攻防作战。研究人员还开发了靶场中的虚拟人类，他们能逼真地测试网络、打开电子邮件，运行应用程序等。

第六个功能是能够测试并评估网络的复杂性。该靶场能在复杂网络环境中进行定性与定量的、无偏差的网络保障能力与生存工具的评估。通过评估能使用户更好地理解复杂系统中出现的异常，检验靶场及其开发使用的研究成果以及网络测试能力。

#### 4. 预期试验和技术能力

美国国家网络靶场还将在以下试验和技术能力方面取得突破：

(1) 对先进的网络信息技术和安全系统开展试验。一边试验可一边修改或替换操作系统及其内核，动态更换其他终端部件/工作站以及整体信息技术。

(2) 在局域网上开展安全工具与组件的试验。在试验中可以修改或替换传统的设备、网络操作系统及其网络体系结构。

(3) 在广域网上对系统进行试验。该系统能在各种网络带宽上运行，并可以修改或替换系统、设备以及体系结构。

(4) 可在战术网络上进行试验。其中也可在移动自组织网络等相似网络上试验。

(5) 可对新的协议进行试验。

### 4.3.2 实施计划与任务

美国国家网络靶场项目分4个实施阶段，其实施计划如图4-10所示。

#### 第1阶段：进行方案设计

这一阶段的开发工作从2009年1月到9月共9个月，其中初步设计评审不超过6个月，主要工作是初始概念设计，提供完整的工程细节和详细的工程计划，制订系统演示计划，并定义操作概念，以及为下一阶段工作提出建议。

系统和概念设计涉及国家靶场设施和信息系统的详细布局及能力、靶场用途、人员发展空间、风险分析、策略优化、项目目标、系统软件、网络架构、系统设计功能和能力等。在工程设计过程中要充分考虑评估进度、设计和测试方法的技术充分性、测试需求、软件

需求，并使之相互衔接并兼容。提供的技术发展计划要适应靶场能力的不断更新。靶场的运行方案应提供安全与试验的流程与管理、资源与试验计划管理、冲突处理与人员需求等。在这一阶段，还要制定操作概念、下一阶段及靶场原型系统详细开发方案。

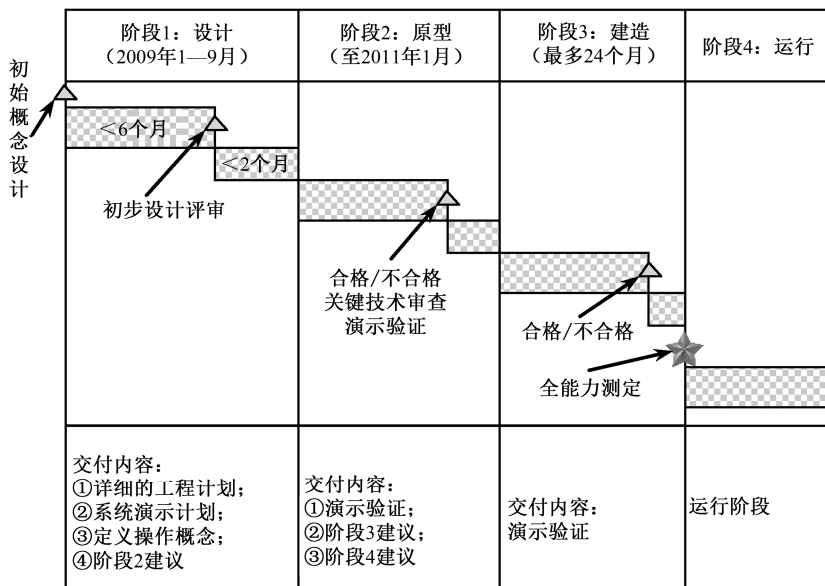


图 4-10 美国国家网络靶场实施计划

该项目第1阶段开发工作由7家承包商分担，其中斯巴达公司获得研制经费860万美元，约翰·霍普金斯大学获得730万美元，洛克希德·马丁公司530万美元，国际科学应用公司280万美元，通用动力公司190万美元，诺思罗普·格鲁曼公司34.4097万美元，BAE系统公司330万美元。

第1阶段结束时，承包商提出的项目计划、系统方案及第2阶段方案必须切实可行、且风险可控，并保证第2阶段项目连续有效地开展。

## 第2阶段：主要工作是建设靶场原型

第2阶段的计划时间约15个月。在第1阶段的基础上，第2阶段建设工作由DARPA选择一个或多个承包商承担，主要完成关键技术审查，制定详细的工程图表，优化并执行工程计划，构建靶场的原型系统，并对原型系统进行演示、仿真和验证，要求承包商尽量降低第2阶段建设成本。还要提出阶段3与阶段4的建议。

关键技术审查的主要目标是：新旧配置方案的演示及部署、实验平台的快速重构、试验管理和时间同步及监控的演示、数据采集工具和流量生成系统的演示、基于人类复制品的演示、飞地间通信信道和所有节点集合的演示、大型实验/试验平台的运行、动态释放测试资源的演示等。

在第2阶段结束的时候，承包商必须演示系统整体及各组成部分的性能，提出廉价的切实可行的方法降低风险，并最终通过DARPA的验收，以保证第3阶段的后续工作。

### 第3阶段：主要工作是靶场建造

在第3阶段，DARPA 首先选择一家承包商进行靶场建设与评估，要完成的工作主要有：

- (1) 物理设施、安全设施和公用设施等所有必要资源的建设；
- (2) 用户、设备配置、试验、设置、应用程序、操作系统、协议、数据文件和安全控制等关键要素和配置方案的生成；
- (3) 采用一定的技术手段保证如联网设备、入侵探测和防御系统、防火墙、VLAN 和安全套接层 (SSL, Secure Socket Layer) 等靶场基础设施与未来网络技术相衔接、相兼容和相配套；
- (4) 利用多种防御技术和手段保护网络安全，提出反病毒测试、加固主机安全系统的策略；
- (5) 研究并开发新的靶场协议与软件，使之满足未来协议和服务的需要；
- (6) 提供启动工作站应用程序的自动化软件；
- (7) 开发出安全管理规定、靶场操作规程、试验安排以及运行方案；
- (8) 借助管理工具对靶场资源进行高层次规划，监控试验过程，完成试验计划制订与执行、数据采集和测试样本管理、试验后分析和关闭等。

建立国家网络靶场的具体要求体现在以下几个方面：

- (1) 承包商必须获得授权并通过鉴定，并要求开展并通过大量的系统试验。
- (2) 靶场必须提供大量自动化工具以提高试验效率。
- (3) 靶场根据试验需求和资源优先级能实现资源的自动分配，并能安全快速地释放试验资源。
- (4) 承包商提供的知识管理软件能使更多新技术被靶场采用。
- (5) 国家网络靶场应该集成新的设备和架构。
- (6) 靶场应可以仿真数千个节点的网络及通信系统。
- (7) 支持用户、管理者、官兵、敌人、中立人员等参与试验，并能测试靶场的运行。
- (8) 靶场应能够在所有节点上模拟人类行为和人类复制品，逼真地复制个人和整个网络，让人类复制品产生多个用户之间的事件链表，扮演多个网络用户角色，模拟执行启动、暂停、继续、终止、重置等操作的交互行为。
- (9) 靶场应能够按照要求自动建立恶意软件工具库和防御工具库。
- (10) 靶场能够生成各种复杂的敌军攻防态势和网络活动，以检验和评估攻防能力。
- (11) 国家网络靶场系统应该是可配置和易于使用的，能集成、仿真、复制其他靶场的资源或被测试系统，其中包括广域网、无线电台、联合战术无线电系统、战术卫星通信系统、路由器、交换机、控制器、C<sup>4</sup>I (Command, Control, Communication, Computer and Intelligence, 即指挥、控制、通信、计算机和情报) 系统、卫星及其通信设备、海事通信、战术移动 Ad Hoc 网络、无人机、武器系统、雷达系统、移动设备、物理控制系统等。
- (12) 靶场应能够插入试验平台并进行多次复制，为模板创建功能相同的逻辑实例，准确地生成物理机器的逻辑实例。这里的实例是指运行的软件和中断级、芯片级及外设级

的硬件。

(13) 承包商应遵守《国家网络靶场安全分类指南》及军地政府的规定，要求多个不同密级的试验项目能同时进行，系统防御能力能有效测试，不必要的资源能自动清理。

在此阶段，DARPA 要求承包商和靶场必须完成以下具体任务：

(1) 提交必需的基础设施。靶场的执行者必须提供的网络靶场基础设施示意图如图 4-11 所示，主要有扩展接口、试验方案、网络技术、协议与服务、演示设施、节点复制、运行资源、管理资源与外部整合等资源。运行资源和管理资源是基础。运行资源包括物理设备、公用设施、安全设施、设计人员、运行以及维护人员等方面；管理资源涉及资格认证、作战构想的制定、安全管理、试验进度以及试验过程等方面。核心部分是网络技术、协议与服务以及节点复制。网络技术包括拓扑结构、攻防技术和网络态势感知等技术；协议与服务一般是指路由协议、网络应用协议和 IEEE 802 系统协议等；节点复制就是对链接、硬件、终端、物理与逻辑设备进行真实复制。扩展接口主要用来连接外部系统及设备。

试验 方案	扩展接口		演示 设施
	网络技术 拓扑结构、攻防技术、网络 态势感知技术……	协议与服务 路由协议、网络应用协议、 IEEE 802系统协议……	
	节点复制 真实复制链接、硬件、终端、物理与逻辑设备		
运行资源 物理设备、公用设施、安全设施、 设计人员、运行以及维护人员……		管理资源 资格认证、作战构想的制定、安全 管理、试验进度以及试验过程……	

图 4-11 网络靶场基础设施示意图

(2) 提出靶场管理方案。这方面的任务主要是提供试验的自动规划、进行资源自动配置、安全清除试验资源以及将空闲资源进行组合优化等。

(3) 对试验进行有效管理。这方面的任务主要是：获取试验态势与想定，采集、分析与存储试验数据，对试验运行实行有效控制，对试验资源进行自动配置。

(4) 提供透明的试验仪器、机制和方法。要及时提供获取试验期间实况的仪器、时间同步机制和审核时间同步机制，及时组织现场评估技术小组进行定量、定性评估。

(5) 有现场人员提供技术支持。在试验现场应有大量高技能的网络工程师、靶场和试验管理员、试验组织者、用户、攻防人员、中立者等积极参与并及时做出响应，还能够真实地复制出人的行为。

(6) 提供系统的可扩展能力。使国家网络靶场与外部系统、敌我网络系统、设备、虚拟机、中间通信媒介，以及其他靶场连接并集成，并且能快速嵌入到试验床中。

(7) 提供加快/减慢试验运行速度的能力。不但要求在统一基础设施上同时进行多项独立的实验，而且在试验过程中能够根据需要加快/放慢运行速度，修正可控的测试时钟。

(8) 确保系统运行安全。确保靶场在各种不同保密级别下试验运行，确保安全地试验恶意软件和恶意代码，确保数据不会在试验中泄露。

(9) 提供逼真的模拟与测试。对攻防试验、多种行为、多种要素、多种网络、多种人员进行逼真的模拟。实现针对互联网/全球信息栅格、各种网络、各种靶场等进行全方位严格的逼真测试。

#### 第4阶段：对运行进行管理

在第4阶段，做好运行的各项技术准备，检验国家网络靶场所具备的能力。这一阶段计划12个月，美国政府答应延长12个月以完成其他工作。该靶场已于2012年10月完成并移交给了美国国防部试验资源管理中心。

### 4.3.3 建设方案

国家网络靶场旨在通过构建虚拟网络试验环境开展网络空间作战与其他网络威胁的试验，以避免对真实物理网络造成破坏。为达到该目标，普渡大学提出了三种NCR建设方案，其中方案I基于虚拟化技术构建，方案II是基于云计算技术，方案III是综合利用前两种技术构建。

#### 1. 方案I

采用不同种类的虚拟化，如硬件虚拟化、直接硬件访问和硬件模拟等，可通过分别安装VMware、Xen和QEMU等虚拟软件来实现。为了部署网络，首先需要设计一个真实的物理网络，然后在物理网络的基础上构建一虚拟网络作为NCR的试验平台。

真实物理网络由Xen/QEMU服务器组成，成为虚拟网络的构建基础，即虚拟网络自身部署于物理网络之上，其包含在NCR中部署不同场景时所需的设备。例如，在图4-12所示的某服务器上可以虚拟出一个完整虚拟网络环境（如大学、企业）。

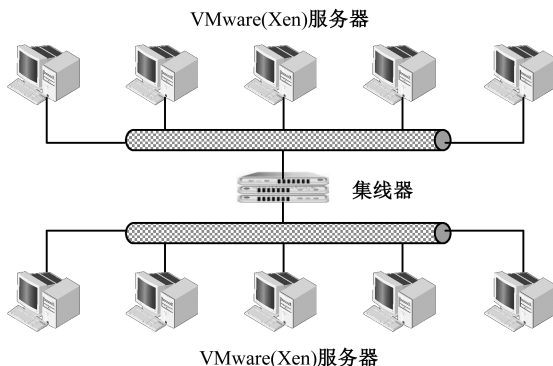


图 4-12 虚拟网络拓扑结构示意图

NCR 需要采用多种不同虚拟设备，安装各种不同操作系统的虚拟机（VM，Virtual Machine），例如 Linux 和 Windows 等。同时包括不同种类的威胁库，如病毒、木马和恶意

软件等，这些威胁同样也是基于虚拟化的，且任意服务器能够虚拟出虚拟主机、虚拟存储、虚拟输入输出、虚拟路由器和虚拟接入点等设备。

NCR 中每个服务器的真实拓扑可能并不相同，例如，可以是网状、环形、总线型和星型结构，以及局域网、广域网、城域网与无线局域网等，从而允许在 NCR 中根据不同的攻击因素配置不同类型网络。NCR 中的数据终端设备（DTE，Data Terminating Equipment）可以是物理设备，也可以是虚拟化的。对于虚拟化的 DTE，大型服务器可容纳所有的虚拟设备，以一种无源头的模式进行远程访问。

为了在 NCR 中产生网络行为，可采用不同的方法。一种是采用人工智能方法，例如网上冲浪。另一种是根据人在网络环境中的活动来产生网络行为。这两种方法用于不同的测试试验中，但是应能模拟不同层次的智能活动，可以通过采用不同层次的人工智能以及不同技能的人来实现。

为了更好管理 NCR，可以采用不同方式，一是在主服务器上监视 VM；另一种是采用不同类型的管理工具、取证工具，用于从 NCR 收集数据，这些工具不仅可用于监视 NCR，而且可重新恢复系统以及清除状态。

## 2. 方案Ⅱ

该建设方案主要基于云计算技术来构建虚拟网络环境。在图 4-13 中，遥感设备、试验导演设备与重置装置在防火墙之后形成一线设备，用于接收数据并将数据发送到虚拟网络中，遥感网将通过一个特殊端口接收数据，收集并用于试验，这些数据可通过中继器仅发送至试验导演设备，以确保在重置机制启动前维持相关事件继续执行。

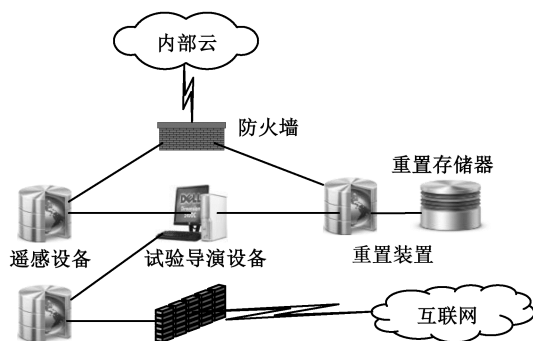


图 4-13 双重云信息间核心系统

重置装置也在一个端口上工作且与试验导演设备共享该端口，因为试验导演设备有能力开始、停止与暂停仿真，且在重置装置启动之前接收已停止试验的设备回复。试验导演设备有能力加载当前未激活的设备，并使之处于激活状态，重置存储器，通过分配的存储空间构建网络，根据试验导演命令发送数据。

在图 4-14 中，内部云被分解为八个主要的部分，能够扩充或收缩成环形信息网。主交换机上安装了重置存储器，所有主要部分都安装在主交换机上。两个大的链接分别连接到主交换机上，其中一个连接到主防火墙并传输遥感信息与试验导演信息；另一个用在试验的终端（设备）用户上。主要的核心设备层被分解成几个分布式云设备。



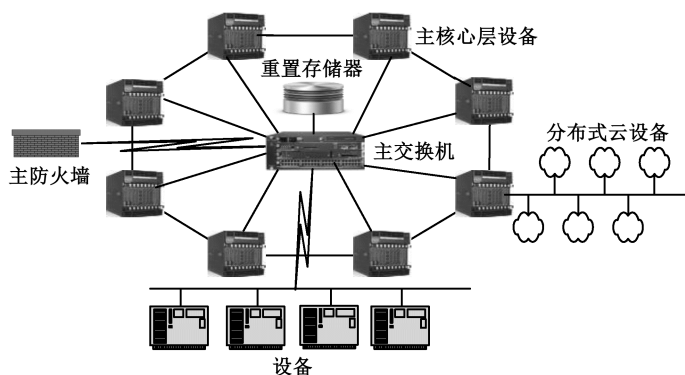


图 4-14 可扩展的内部核心层系统

在图 4-15 中，分布式云系统以物理总线方式组织，但能够被虚拟化成任意的组织方式。第一层分布式结构包括虚拟网关、虚拟路由器、虚拟链接和虚拟交换机。第二层是真实主机，这些主机将能够构建各种不同的虚拟化终端设备，由这些设备中某些部分可构建黑客网。其中每一个主机设备应有一个重置系统来加快重置时间，采用 VMware ESX 软件为虚拟机加载脚本和操作系统镜像。在试验导调方的控制下，主机设备能够加载、创建与删除设备。小型的虚拟应用能够部署在主机系统上，使得整个设备变成恶意设备。

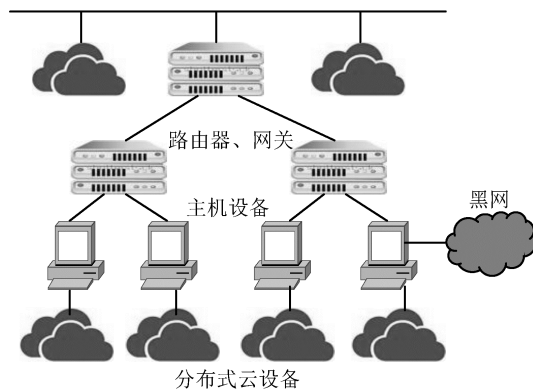


图 4-15 可扩充的分布式云系统

### 3. 方案Ⅲ

将前两种方案组合成一个多异构设备的集群。在原型系统中，拥有 241THz 的处理器设备，其随机存取存储器（RAM，Random Access Memory）大小为 128~512MB，使得正常的原型系统能快速扩充且无额外开销，对试验参数要求更加严格。与正常环境相比原型系统环境的逼真度较差，但能提供大量设备。在外部校园网络参数的限制下，才可真正利用网络。通过最大/最小协议分析测试，查看其是否真实有效。

集群信息的星型拓扑结构要优于网状拓扑结构，对原型机而言，星型拓扑结构用于中心路由器，中心路由器再连接一个或多个路由器。需要考虑在低层采用 VMware ESX 软件

实现多种设备的虚拟化, ESX 通过采用 Vyatta 软件在一个主机操作系统上实现多设备的虚拟化功能。图 4-16 显示了一个小型分布式系统能够容纳多种设备, 从底层到上层, 网络附加存储(NAS, Network Attached Storage)方式/存储区域网络(SAN, Storage Area Network)设置重置参数类似于加载虚拟机与脚本。这可以看作主要的数据存储基于并行的信息处理原理来实现虚拟化功能, 包含遥感设备, 该设备应通过防火墙与外部网络设备分离, 尽量减少由输入/输出引起的内部/外部系统与网络之间的冲突。

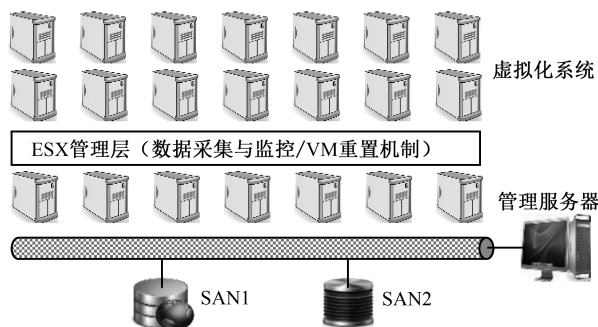


图 4-16 使用 ESX 管理异构集群的虚拟设计方案

#### 4. 三种方案比较

在方案 I 中, 靶场的虚拟网络环境是在物理网络基础上的, 通过部署各种虚拟化实例而构建, 其建设成本较低, 能够根据靶场不同试验对象建立不同结构和组成要素的网络试验环境。其不足之处在于: 为实现靶场的灵活高效管理, 需针对不同的靶场试验对象/试验任务开发不同类型的管理工具, 导致其可扩展性和灵活性较差。

方案 II 中采用了遥感器、测试导演等设备接收外部真实数据并发送到仿真网络环境中。相对于方案 I, 其构建的靶场环境逼真度较高, 但相应的建设成本也较高。该靶场环境中的内部核心云可通过主交换机与外部网络或终端测试应用相连接, 从而具有灵活的可扩展性, 能够将外部网络、设备统一整合集成。

方案 III 基于前两个方案的优点, 构造了多异构系统的集群, 该系统可以快速扩展, 并适应于特定参数下的测试试验, 靶场试验的功能齐全; 同时, 系统可与外部网络进行互联互通, 具有较强的交互性。通过云计算平台对底层设备资源的统一管理, 将不同的计算任务分配到集群中不同计算节点上, 从而提高整体计算能力。但是该系统需要建立一个庞大的云计算平台, 导致建设成本增加。

#### 4.3.4 试验特点与流程

经过 2009 年 1 月至 2012 年 10 月近四年的建设, 美国国防预先研究计划局于 2012 年

10月将位于洛克希德·马丁公司设施内的国家网络靶场移交给了美国国防部试验资源管理中心。目前,国家网络靶场已具备了开展试验与训练的能力。据美国国防部称,国家网络靶场已被用于对一个模拟了15 000个高保真节点的网络进行了试验。靶场在2012年承担了近10项网络试验任务,并逐步承担了更多的网络试验任务。

### 1. 主要特色

国家网络靶场是美军最大的网络靶场,可以模拟互联网等大型网络,其特色主要体现在以下四个方面:

(1) 体系结构安全可靠。采用安全架构,可以同时进行多个密级不同的试验,从而使靶场的利用最大化。靶场先后进行了绝密/敏感隔离信息(TS/SAP级)、敏感隔离信息(SCI级)认可和认证测试。

(2) 试验设计简便易行。试验设计工具能够使用户快速设计网络拓扑结构和具体的试验。这些工具也可以在用户所在地运行,从而提高了网络试验的可达性。

(3) 靶场配置自动高效。通过硬件和软件工具,可以自动配置靶场,构建环境,进行试验。这大大缩短了试验周期,将配置靶场进行试验的时间从数月减少到数小时。

(4) 复位还原自动进行。在试验后靶场可以自动还原复位,并在任何密级下重新使用,这样,可以加载新的代码并进行试验,而不会给靶场带来危害。

### 2. 试验过程

在国家网络靶场进行网络试验的过程执行六个步骤。该过程始于一个通用的、汇集了相关资源和网络工具的硬件和软件池。试验结束后,可以重新进行先前进行的试验,或进行新的试验。图4-17给出了美国国家网络靶场试验流程图。

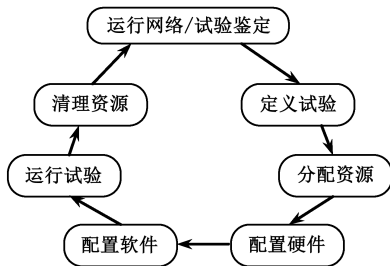


图 4-17 美国国家网络靶场试验流程图

国家网络靶场试验过程的六个步骤为:

- (1) 定义试验。利用具体的试验工具来定义端对端情况。
- (2) 分配资源。自动调度程序,调用并分配硬件和软件池中的资源。
- (3) 配置硬件。配置工具自动将硬件连接到相应的配置上。
- (4) 配置软件。配置工具自动配置和验证进行试验所需的软件。
- (5) 运行试验。试验团队验证环境,安装被试系统,运行试验,采集数据。

(6) 清理资源。整理、净化硬件，并虚拟地将硬件/软件资源放回到硬件和软件池中。

### 4.3.5 网络靶场能力发展思路及体系框架分析

从国外网络靶场建设和承担的任务来看，网络靶场的主要使命是模拟网络空间攻防环境，为网络空间对抗技术和装备的试验鉴定、效能评估、人才培养，以及国家网络安全检验提供可靠的场所。

美国国家网络靶场不是进行全新技术理论科学研究或成熟技术测试验收的场所，它更多关注的是有一定理论基础但还不够成熟的网络空间技术。在这里，研究人员通过科学的实验和严谨的测试来验证相关技术的可行性，并可以对该技术进行初步的开发，美国国家网络靶场关注范围如图 4-18 所示，网络靶场重点关注的是技术成熟度处于 3、4、5 阶段的技术。

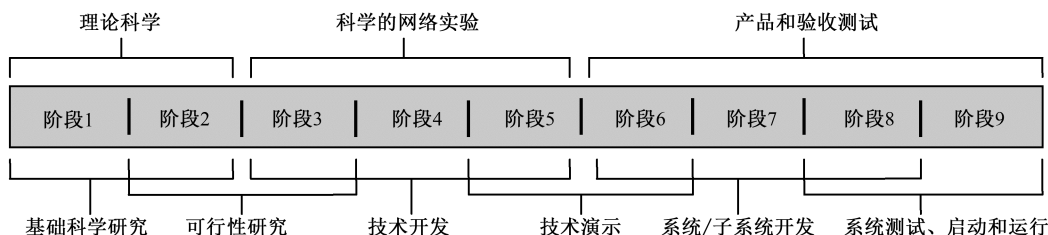


图 4-18 美国国家网络靶场关注范围

美国国家网络靶场将成为一种测试涉密与非涉密网络空间项目的国家资源，它能够为特定实验分配资源，建立实验平台，协调安排靶场测试时间与测试资源，它将支持多任务测试、同步测试、单元测试，以及相关的测试平台。美国国家网络靶场与传统的电子靶场、通信靶场相比，具有明显的特点和优势：将使用大量新技术；能复制当前和未来国防部武器系统和作战中复杂的、大型的异构网络 and 用户，实验规模更大；能够在不同安全级别下同时进行多项独立仿真实验，具有封闭与隔离测试、存储的能力；通过专门的工具软件和技术能够对实验参数进行自动化快速配置，并允许用户对靶场资源快速重复使用，实验周期更短，实验结果更准确；用户体验更加具有真实感；能够加速和减缓相关测试时间，方便用户对实验进行分析；能够生成用于知识管理、存储测试用例和历史经验的知识仓库，可为未来工作提供帮助。

随着网络化系统的飞速发展，传统的测试手段和技术已经无法满足对新型系统的测试需求，且测试技术领域的空白还在不断扩大。美国国家网络靶场项目很好地填补了这个空白，该靶场是一种对预期作战环境的仿真，包括通信网络拓扑、网络设备、通用计算机、加密设备、特殊用途数码硬件，以及安装在这些硬件上的所有软件；靶场还包括用于模拟内部和外部数据的流量生成工具、完整的恶意软件库，以及用于模拟网络攻击和防御行为

的工具库。美国国家网络靶场比传统的测试手段提供了更高精度的检测和评估环境,使得待测系统能够在更深更广的范围内得到评估。

美国国家网络靶场具有明显的三层体系架构,原型靶场体系架构如图 4-19 所示,从上到下分别是靶场资源接口层、靶场运行层、用户测试层。

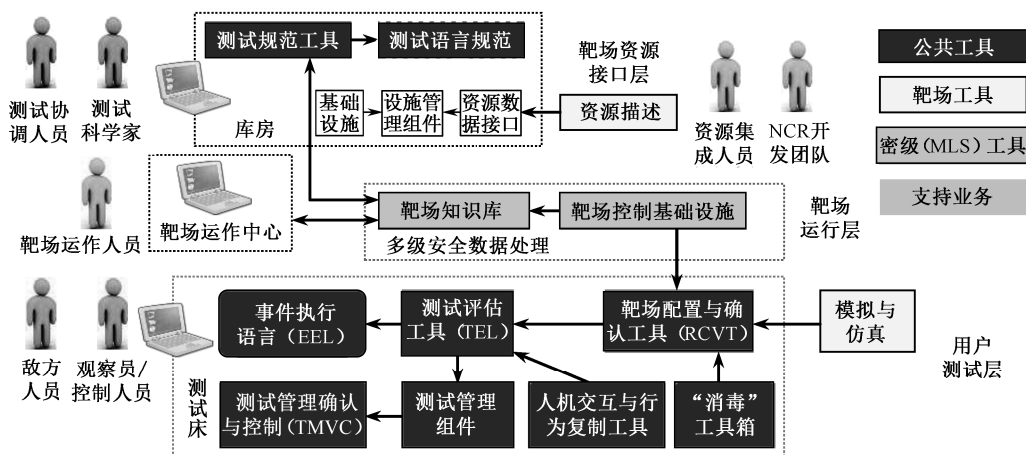


图 4-19 原型靶场体系架构

靶场资源接口层是整个美国国家网络靶场的基础,它为用户提供大量的具有统一语言规范的资源接口服务,它是由构成靶场的基础设施、资源数据接口、测试语言规范以及用于管理靶场知识库的设施管理组件和测试规范工具的套件组成。该层中提供的网络科学测试语言是整个网络靶场开展实验的基础,网络科学测试语言将贯穿于一个完整的网络实验生命周期中,在实验设计阶段,网络科学测试语言将帮助实验人员为实验开发一套统计学设计方案,明确实验目标、实验类型、实验相应变量、资源描述、资源调度等细节,在国家网络靶场中,对资源的描述是通用的、独立的、分层次的,能够在不修改代码的情况下增添新的设备资源;在实验执行阶段,使用了网络科学测试语言规范的靶场软件能够自动生成虚拟化节点和测试平台,并通过插入测试活动来进行实验;实验结束后,实验结果将会以网络科学测试语言的格式生成,以方便数据分析和数据归档,同时实验变量将会被相应的脚本自动清除。

靶场运行层是整个靶场运行的关键层,它负责接收来自用户测试层的实验需求,并通过向靶场资源层调取相应资源来自动进行仿真实验,并最终将仿真实验结果反馈回用户测试层,它是由靶场控制基础设施和靶场知识库组成的。靶场控制基础设施负责仿真事件的协调和资源调度,通过控制用户测试层的各种工具来保证各种执行脚本的顺利运行并生成和监视网络流量。

用户测试层是对用户可见的层,该层为用户提供了友好的操作界面,方便用户完成资源调用和仿真模拟过程,它是由靶场配置与确认工具、测试评估工具、事件执行语言、测试管理确认与控制、测试管理组件、人机交互与行为复制工具、“消毒”工具箱等组成。实验之前,用户可对这些工具预留的参数接口进行配置,实验运行时靶场运行层的靶场控

制基础设施将对这些配置好参数的工具进行自动调用，该层的这些仿真软件是以 Emulab 软件为基础发展而来的。Emulab 是一个应用于网络和分布式系统领域的仿真测试实验平台，能够为研究人员提供多种环境来开发、调试和评估他们的网络和分布式系统，洛克希德·马丁（Lockheed Martin）、Sparta、ISI 等企业在进行网络仿真模拟时使用的都是 Emulab 软件。

以靶场资源接口层、靶场运行层和用户测试层的三层体系架构为基础，在模拟实验时，网络靶场可以提供一个可控、可预测、可重复的环境，包括可以完全访问的个人计算机节点，运行在所选择的操作系统之上，允许用户指定一个任意的网络拓扑结构。

4.3.6 使用的最新技术和方法

国家网络靶场为美军模拟真实的网络攻防作战提供虚拟环境，针对敌方对电子攻击和网络攻击等作战手段进行试验，测试各种网络技术革新。美国国家网络靶场的相关技术可以分为三个领域：网络靶场基础构建、网络靶场管理和网络靶场实验管理。美国国家网络靶场最新技术特点见表 4-2。

表 4-2 美国国家网络靶场最新技术特点

类 型	使用的最新技术和方法
网络靶场基础构建领域	网络科学方法；网络科学测试语言规范架构；资产鉴定方法；资产描述规范和数据库规范；安全管理设计方法；运用了统计学方法的实验设计方法；网络配置的输入方法；利用附加议定书、服务和网络的杠杆作用
网络靶场管理领域	知识库管理套件；设备管理套件；教学培训知识库管理套件；实验规范工具；自动化实验规划技术；自动化资源分配技术；实验结束后的快速安全资源释放技术；高效而免费的“资源池”技术；“数据擦除”工具箱
网络靶场实验管理领域	自动化靶场配置、验证和实验技术；数据采集工具；自动化实验控制与管理技术；自动化实验分析与演示技术；先前实验结果与数据分析技术；半自动化进攻与防御工具库；自动化实验重构技术；实时人机交互技术

网络靶场基础构建领域的相关技术是最基础的技术，主要以科学的实验研究方法以及相关的规范和标准为主，测试语言、数据库、测试资源和配置的规范化、标准化将贯穿于一个完整的网络实验生命周期中，有利于网络电磁实验的模块化、自动化和易扩展性。其中，网络科学测试语言能够用于描述实验设计、实验模板、待测试网络、测试计划、执行细节和数据分析，测试规范和报告通过网络科学测试语言的规范化表达，方便了知识管理和结果分析。资产描述规范则定义了在网络电磁实验中的硬件和软件资产，对硬件资产的描述是通过基于组件的方法来实现的，主要描述了该组件能够提供给测试平台中其他资产的功能；对软件资产的描述则与其传输或下载的特定字符串有关，主要描述了软件资产在

测试平台中的功能、所依赖的通用功能、相应的补丁和安全更新等。

网络靶场管理领域的相关技术能够使靶场管理人员对靶场的软件、硬件基础设施和知识库等资源进行高效、安全和自动化管理。

网络靶场实验管理领域的相关技术能够让实验用户对网络靶场实验过程进行自动化配置、监视、控制、分析和重构。

建设 NCR 时面临的关键技术难点主要有：大规模网络仿真环境构建技术、靶场试验时钟同步技术、靶场试验运行控制技术等。

### 1. 大规模网络仿真环境构建技术

NCR 需要能够重现出大规模的军事、政府和商业网络，由于网络的规模庞大、覆盖范围广，形态多样且动态变化，靶场难以利用有限的物理资源真实重现各类网络。故需要采用仿真的方法以扩大靶场的规模，且尽可能减少与真实网络环境的差异性，同时根据不同的试验要求和对象按需部署，以满足靶场试验环境在结构、规模和节点要素等方面的要求。

### 2. 靶场试验时钟同步技术

在 NCR 中进行试验时，为提高试验的逼真度，通常需要将外部的实际设备与系统作为配置测试系统接入靶场。由于这些真实资源与靶场中的虚拟资源在时钟同步方式、描述精度与运行方式等方面存在差异，而且在大规模网络环境中存在不可预知的网络延时，故需要解决真实资源与虚拟资源之间的精准时钟同步问题。

### 3. 靶场试验运行控制技术

网络靶场试验运行控制技术主要包括试验的进程控制和调试控制技术。其中，试验进程控制技术主要包括进程的开始、跳转、加减速、冻结、恢复和结束等，试验过程的缩短与延长是通过运行不同粒度的时间驱动来实现的。试验调试控制技术主要通过调整试验设定中的事件顺序来完成的。

## 4.4 美国几种典型的网络靶场的建设情况

### 4.4.1 国防部信息确保靶场

2009 年 10 月，位于美国弗吉尼亚州斯塔福德匡蒂科海军陆战队基地附近的国防部信息确保靶场初步建成并投入使用。靶场主管部门为美国国防部国防信息系统局，实际运营部门为海军陆战队司令部指挥、控制、通信与计算机处。据美国军方称，国防部信息确保

靶场这一网络空间“沙盘”可以模拟 GIG，进行网络试验鉴定和训练演练。靶场可以用作独立的模拟器，也可以与各作战司令部、各军种和国防部各机构的其他靶场连接和互操作。美国国防部信息确保靶场拓扑结构图如图 4-20 所示。

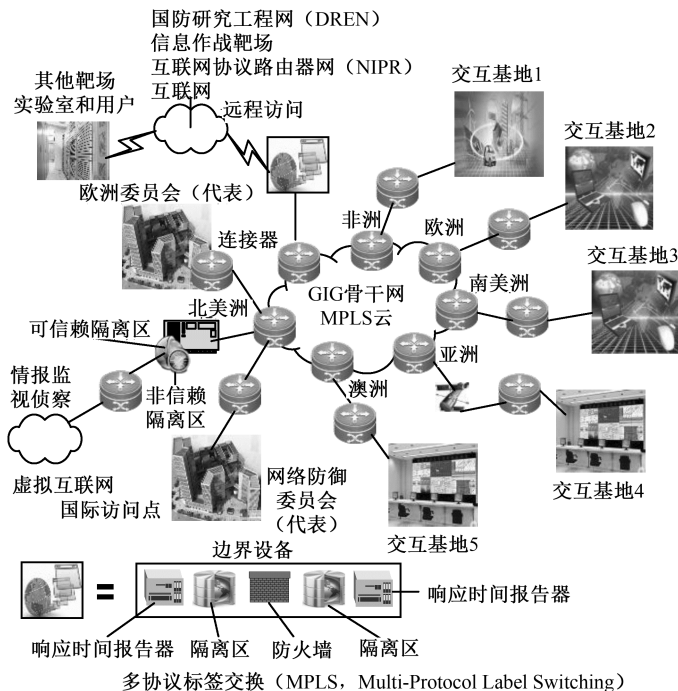


图 4-20 美国国防部信息确保靶场拓扑结构图

## 1. 靶场环境

国防部信息确保靶场基于开放式体系结构设计，可以通过配置为个体训练演练需求提供支援。这种灵活性包括诸如通信流量生成、威胁注入、操作系统类型、补丁等级、飞地机器和网络服务等细节。这一环境还可以对企业信息确保设备和应用软件进行测试、鉴定，以及对互操作性做出评估。为了模拟逼真的作战环境，国防部信息确保靶场采用了诸如系统管理员模拟训练器和“突破点”工具等。

国防部信息确保靶场提供的环境为通用的美国国防部一级至三级建模与仿真环境。靶场可以提供由恶意和友好网站组成的虚拟互联网。据美国国防部国防信息系统局称，可以从虚拟互联网向国防部信息确保靶场的 GIG 环境发动模拟的威胁攻击和真实的“红队”攻击。

2012 年 7 月，靶场建立了一个与非保密 GIG 环境相同、可以在秘密级运行的环境。在此环境下，可以开发和演练秘密级战术、技术与程序，可以纳入秘密级防御或攻击工具，可以运行秘密级作战想定。该保密环境采用了保密协议路由器网和骨干网。2013 年，靶场拥有了可以运行绝密/敏感隔离信息 (TS/SCI) 级的环境。



## 2. 主要职能

国防部信息确保靶场结合纵深防御战略的设计原则，为美国国防部各组织机构提供了一种井然有序、可重复、可验证的网络试验与鉴定架构，可以用于度量网络防御人员的能力，有机整合人员、行动和技术，对网络安全攻击进行防护、监测、探测、分析、诊断并做出响应：遏制、消除并从中恢复。作为一种能力，国防部信息确保靶场除了提供一种从作战环境中分离出来的逼真的试验与鉴定环境外，还为美国国防部各组织机构提供一种度量网络安全人员作战能力、现有网络安全服务充分性的途径和手段，并验证已确立和批准的信息确保和计算机网络防御战术、技术与程序。

### 4.4.2 联合网络空间作战靶场

联合网络空间作战靶场是美国国防部的主要网络靶场之一，可以为网络空间作战人员等提供在逼真的环境下进行训练的能力。靶场位于伊利诺伊州斯科特空军基地。靶场由康贝公司（Camber）（代表空军）负责维护和运营。靶场充分利用仿真技术来支持作战人员进行全面的训练、培训、认证和军事演习，允许用户连接分布在各地的各军种或机构的网络训练系统，使用户通过靶场获得网络保护、防御和作战等方面的作战经验和能力。

2011 年，靶场用户累计登录模拟器的时间达 30 548 小时。截至 2012 年 11 月 1 日，已累计登录达 34 788 小时。目前，美国空军官员正在采取措施，以进一步扩大靶场的用户。另外，靶场的用户类型也发生了变化。用户不再仅仅是空军人员，还包括来自其他作战司令部、军种、学校和机构的人员。用户也不再仅仅是传统网络领域的用户，还包括负责搜集敌方情报信息的情报人员等。

#### 1. 基础设施

联合网络空间作战靶场拥有 13 种不同的模拟器，其中有些模拟器具体到某个网络层，如基地级计算机网络、空军级计算机网络等。靶场主要基础设施包括部分任务训练器、互联网仿真能力设备和信息数据库等。

##### 1) 部分任务训练器

可用于对具体的任务进行训练，如防火墙或电子邮件流量管理等。部分任务训练器可以针对具体需求对仿真进行裁剪，使训练拥有更多的选择，如在飞机模拟方面，可以只模拟带有炸弹架的机翼，而不是模拟飞机的一切，这样，可以不用考虑动用较大的靶场，如基地级靶场或第二层网络。

## 2) 互联网仿真能力设备

互联网仿真能力设备亦称“非动能合成轰炸靶场”或“环球靶场互联网”，它可以使网络防御人员从位于世界各地的军事基地登录并进行训练。

## 3) 信息数据库

信息数据库拥有构造仿真模型，可以为模拟训练提供信息，使参训人员拥有空中的虚拟人员或虚拟机器，以及“环球靶场互联网”上的虚拟网络等。

## 2. 主要职能

联合网络空间作战靶场可以用于网络实兵训练（如战斗机飞越训练靶场）以及虚拟仿真训练和构造仿真训练。其最初的使命任务是支持每年相对较少的网络演习，但靶场现在可以提供持续的训练和培训，并支持每年进行大量演习。另外，靶场最初只用于对相对较少的防御作战人员进行训练，但靶场现在增加了攻击性作战训练。不断变化的任务还包括支持动力学事件的网络作战训练。

联合网络空间作战靶场源于空军训练演练模拟器（SIMTEX）项目。根据美军设想，每个军种都要拥有类似于 SIMTEX 的项目，这样，军方的模拟器就可以连接在一起，进行联合网络训练。美军将联合网络空间作战靶场描述为一个靶场联盟，除 SIMTEX 靶场外，靶场联盟的主要成员还包括海军网络空间作战靶场、战略司令部网络作战靶场，以及陆军国民警卫队增强型网络训练模拟器靶场等。据美国空军官员透露，联合网络空间作战靶场于 2012 年夏季与美国国家网络靶场进行了集成。

### 4.4.3 海军网络靶场建设思路

#### 1. 总体框架

海军网络靶场的主要任务是研究和开发适用于海战场环境的网络安全仿真试验平台，其总体框架图如图 4-21 所示。研究人员可以根据需要设定网络设备参数、网络拓扑结构、脆弱性参数、威胁参数、拟评估参数等网络攻防参数；根据不同的试验需求，从网络攻防试验模型和试验数据库中选取不同的试验模型和试验数据，进行网络攻防试验。在试验过程中，靶场要能够在运行资源和管理资源之上支持不同攻防场景的快速部署，使得研究人员能够全方位地对靶场和被测系统进行安全性评估，重点完善并改进薄弱环节，研发各种新技术来应对可能的威胁和攻击；靶场要能够进行网络攻防态势感知，测试对比各种态势感知工具的功能和性能；靶场要能够通过设定不同的网络拓扑、网络协议与服务和网络流量，测试并评估网络的复杂性。此外，靶场应支持人为地为被测试系统设置系统漏洞或故

障,以测试被测系统的管理配置安全性。所有的攻防试验数据都被详细地记录下来,通过数据处理和分析,生成便于直观理解的结果,反馈给研究人员、指战员和上级机关,用以评估靶场、被测系统的安全性和抗攻击性,采取的网络攻防手段和方案的优缺点,并进一步形成和丰富网络攻防试验模型和试验数据库。

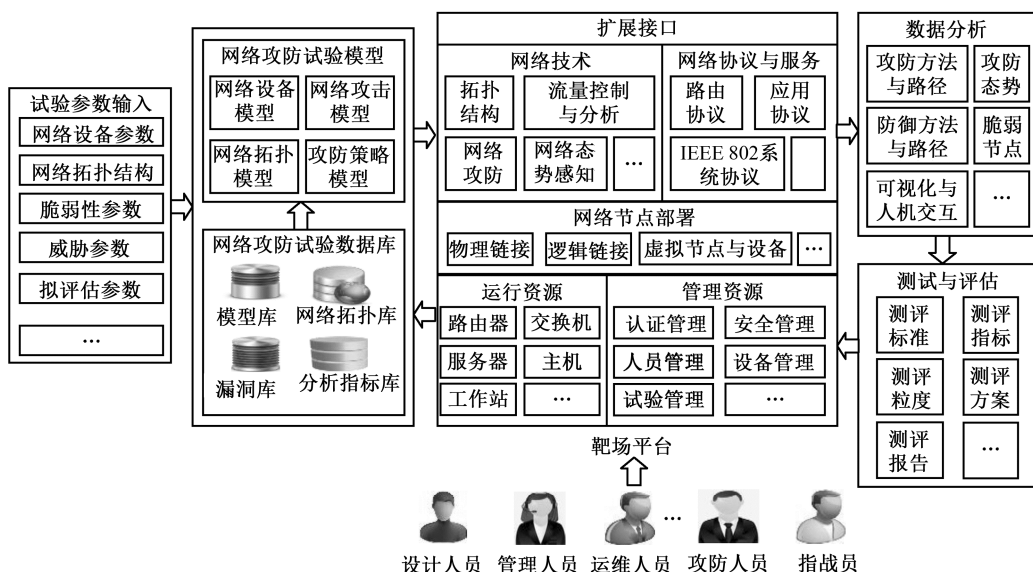


图 4-21 海军网络靶场总体框架图

## 2. 建设方案

海军网络靶场的建设需要不同的技术部门共同参与,需要由统一的部门统筹管理,协调分工,做好靶场基础设施建设规划和标准的制定,统一信息格式和标准化接口,以使靶场内的资源和信息互联、互通、互操作,实现海战场环境下一体化的试验功能、机动化的试验平台、多样化的试验模式、精确化的试验指挥、可视化的试验场景。在靶场的建设过程中应重点考虑以下方面:

- (1) 尽可能重现真实的物理网络状况,包括路由器、交换机、服务器、防火墙、入侵检测设备、无线接入设备等要素。
- (2) 尽可能全面反映各种平台和服务的工作状况。
- (3) 尽可能包含具备不同安全意识等级的网管人员的管理策略和方法。
- (4) 尽可能详细地记录各种攻防日志,提供数据处理和分析功能,把处理后的攻防数据以直观的方式展现给研究人员和指战员,便于反馈和学习。

在靶场建设过程中,可从靶场平台、网络攻防、数据分析、测试与评估等几个方面来具体实施,包括:提供基础平台和软硬件环境,设定相应的版本和补丁可控的操作系统以及各个系统平台漏洞;网络上提供各种协议服务和应用软件,允许数据在网络上以明文方式传输,同时也提供数据加密和完整性校验机制,允许/禁止网段内数据包过滤和嗅探,允

许网络欺骗和中间人攻击等，各种级别的访问权限控制，人为的管理漏洞，如弱口令、口令重用、敏感文件无规范放置；详尽的攻防日志以及机器状态日志；等等。

### 1) 靶场平台

网络靶场需要提供近似真实环境的仿真环境，可通过云计算技术搭建基础平台。云计算通过网络将超大规模的计算与存储资源整合起来，并将计算任务分布在这些资源池上，使用户能够根据自己的需要获得计算和存储等信息服务。云计算将抽象的业务逻辑与具体的计算资源分离，用户只需关注自身的业务逻辑，而无须关注复杂、易错的底层计算机的资源管理。这些特点使得采用云计算技术构建网络靶场时能做到低成本，容易管理。

每次进行靶场试验前，可动态地创建虚拟机以满足当前试验所需要的节点数量，并通过对虚拟机的灵活部署和动态迁移，形成预想的网络拓扑结构。靶场试验过程中，所有的攻击效果都被限定在虚拟机中，对实际的物理设备的影响甚小，减少了物理设备因攻击而出现故障或损坏而需要增加投入的风险。每次试验结束时，可动态地挂起或者销毁虚拟机，释放分配的试验资源，由靶场完整回收并供下次试验继续使用。研究人员可以非常方便地在靶场中部署各种不同的攻防场景，反复演练不同的攻击和防御手段。

### 2) 网络攻防

网络靶场在建设和运行过程中，需要反复演练各种网络攻击和防御手段与策略，测试发现漏洞和攻击点，试验改进新的防御工具，同时也在攻防演练的过程中提高相关人员的网络安全防御意识和能力。

网络攻击一般包括三个阶段，即攻击的准备阶段、实施阶段、善后阶段。在准备阶段，主要是确定攻击目的，侦察扫描目标系统，准备攻击工具。在实施阶段，攻击者首先会隐藏自己的位置，然后利用收集到的信息和各种手段登录目标主机并提升权限，之后便是利用漏洞、后门或其他方法获得控制权。在善后阶段，攻击者需要消除或者隐藏攻击痕迹，植入后门或木马，退出目标系统。攻击者通过远程控制植入的后门程序或木马，可以随时再次对目标系统发起攻击。在网络靶场的建设过程中应至少考虑以下攻击方式：网络侦察技术，拒绝服务攻击，缓冲区溢出攻击，程序攻击，欺骗攻击，利用处理程序错误攻击，高级可持续攻击等。

在网络安全防护技术方面，可以从网络的不同层次和角度采取不同的安全技术。

(1) 信息传输安全技术：保护传输信道的物理层与链路层，主要包括通信链路加密和数据加密、数据完整性校验、信道的旁路攻击检测和防护等技术。

(2) 信息交换安全技术：保护数据的可靠寻址、路由与交换，主要包括网络实体的身份认证、路由表访问控制、地址反欺骗、协议报文防篡改等技术，以及采用自主设计的通信协议，包括呼叫处理、信令处理、路由协议等。

(3) 网络服务安全技术：保护应用层的网络服务，主要包括应用系统访问控制、拒绝服务攻击检测与防御、入侵检测与保护、安全审计、数据包过滤、深度包检测、反病毒、漏洞扫描与挖掘、虚拟专用网、蜜罐、安全恢复等技术。

(4) 自免疫与自愈技术: 当网络受到攻击而影响到正常的服务功能时, 能够通过自身的免疫能力来实现网络的自愈。

(5) 网络管理安全技术: 保护管理各类网络设备, 主要包括网络管理安全需求的等级划分与保护, 网络管理安全架构与访问控制, 网络资源的保护机制与实时监控, 基于策略的网络管理等。

(6) 网络安全分析评估技术: 用于评定网络的安全防护能力, 针对网络安全策略, 给出理论分析和仿真结果, 结合定性和定量的分析结果, 得出网络的风险评估模型、风险评估方法和网络安全威胁标志, 检测网络的渗透性和安全脆弱性等。

此外, 还可以将一些其他技术应用到网络攻防演练中, 如可信计算技术、博弈论等。可信计算技术能够从底层硬件保护信息系统, 可抵抗软件攻击, 为平台以及运行在平台上的软件提供完整性证明, 从而为上层应用系统提供安全可信的运行环境; 将可信计算技术延伸到网络层面, 可以构建可信网络连接, 对网络用户的身份进行认证。理想的防御系统应该对所有的弱点或攻击行为都做出防护, 但是从组织资源限制等实际情况考虑, “不惜一切代价”的防御显然是不合理的, 必须考虑“适度安全”的概念, 即考虑信息安全的风险和投入之间寻求一种均衡, 应当利用有限的资源做出最合理的决策。因而, 可以将攻击者与防御者之间的攻防过程抽象为一个二人的博弈问题, 防御者所采取的防御策略是否有效, 不应该只取决于其自身的行为, 还应取决于攻击者和防御系统的策略, 从而通过均衡的计算来寻找最优防御策略。

### 3) 数据分析

网络靶场在试验过程中会产生大量的原始试验数据, 这些试验数据是分析、评估和改进靶场和试验系统的关键因素。对原始试验数据的详细记录是一个方面, 更重要的是对试验数据的分析与处理。首先, 需要对大量的试验数据进行预处理和清洗, 去除偏差较大或无效的干扰数据, 使得分析的结果尽可能反映真实的靶场情况。其次, 需要高效的数据分析方法和工具, 如可以通过数据融合算法和技术对预处理后的数据进行融合, 再用数据挖掘技术和机器学习方法对融合数据进行分析, 也可以采用大数据技术处理分析试验数据。最后, 还需要有直观有效的数据解释方法和工具, 方便用户对数据分析结果的使用, 通过数据分析结果能够直观地总结靶场和试验系统当前的状况和薄弱环节, 涉及的主要技术包括可视化和人机交互等。

### 4) 测试与评估

网络靶场建成后, 研究人员可以在靶场环境中对海军的指挥控制、信息传输等信息技术和系统的安全性, 以及信息安全保障工具与手段进行定性及定量的评估。通过对复杂的海战场环境的高度仿真, 既可以在靶场内同时对海军的各信息系统进行独立的测试与评估, 也可以在各信息系统之间进行一体化的联合演练测评, 从而为海军各信息系统的优化改进、提高系统安全性和抗攻击性等提供试验支撑。

海军网络靶场测试对象应涵盖各信息系统的关键组成要素,包括主机操作系统与系统内核、关键设备/终端部件、主机安全系统、局域网安全工具和组件、网络操作系统和设备、网络拓扑结构及网络协议等。为对靶场的实际功能效果进行翔实有效的测试与评估,需根据相应的测评标准拟定测评指标。海军网络靶场的测评标准制定可参考国内外使用广泛的测评标准,如美国的《可信计算机系统评价准则》(TCSEC 橙皮书)、我国的《计算机信息系统安全保护等级划分准则》(GB 18759-1999)、中国人民解放军总装备部的《信息安全保障体系框架》(GJB 7250-2011)等。

#### 4.4.4 联合信息作战靶场

联合信息作战靶场由总部设在弗吉尼亚州萨福克的联合参谋部 J-7 处管理,提供的是一种联合网络空间作战试验环境。靶场是一个闭环、安全、全球分布式网络,该网络构成了与实弹发射相关的逼真网络空间环境,支持各作战司令部、各军种和国防部各机构,以及试验界在信息作战和网络空间任务领域的训练、试验和实验。联合信息作战靶场典型试验体系和结构如图 4-22 所示。靶场可以提供一种削弱或拒止的环境,在这种环境中可以进行战术、战役和战略级训练和试验。除其他机构、国家实验室、工业界和学术界之外,靶场可以与美国国防部以及各军种的网络靶场连接。

靶场的主要任务是在采办周期中对指挥和控制技术设备进行试验。靶场网络通过了美国国防情报局的认证,可以在七个安全等级(从公开信息级到敏感隔离信息级)中对进攻性和防御性网络空间能力进行试验。

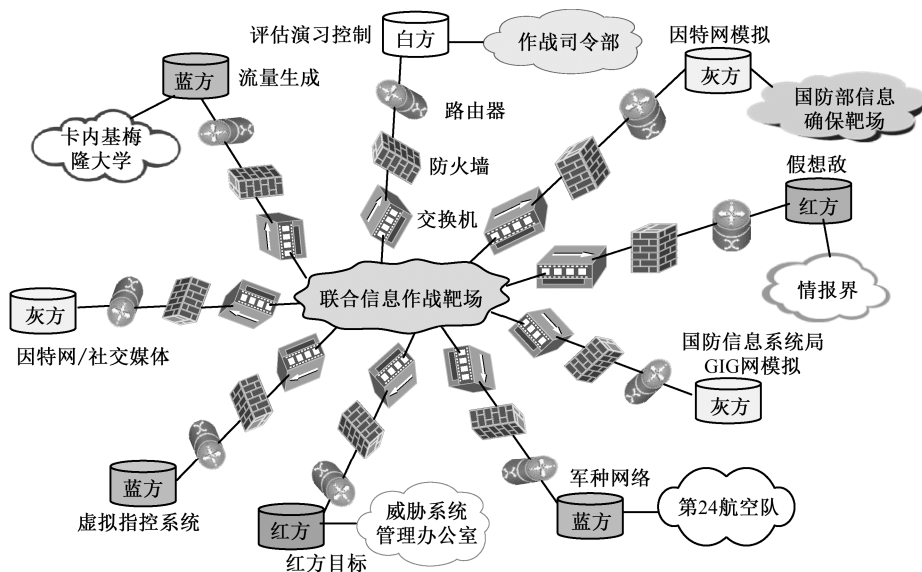


图 4-22 联合信息作战靶场典型试验体系和结构

#### 4.4.5 美军网络靶场建设发展特点

##### 1. 初步形成多靶场并存的格局

美军在网络靶场能力建设上分为不同的层次,既有针对网络战的全功能、高复杂度的大型靶场,如耗资大、周期长的国家网络靶场,又有包括针对当前作战威胁和网络战演练的中型靶场,如国防信息系统局的信息确保靶场,还有各军种各自的网络靶场等。

这些靶场在用户、功能等方面有所不同,各具特色。如在模拟对象方面,美国国家网络靶场主要用于模拟互联网,国防部信息确保靶场主要用于模拟全球信息栅格,而各军种的网络靶场则主要用于模拟各军种的作战、指控网络。不同层次、不同类型网络靶场的同时建设,可以满足不同领域对网络空间作战能力的需求,能够有效推动网络空间作战能力的全面发展。

##### 2. 能够进行多靶场联合试验训练

与其他武器靶场发展建设道路一样,在网络靶场运行使用方面,美军依然坚持走“无边界靶场”的路子。美军的各网络靶场既可以独立运行,又可以联网运行。目前,美军网络靶场联盟已初步形成,靶场联盟主要成员包括空军训练演练模拟器靶场、海军网络空间作战靶场、战略司令部网络作战靶场,以及陆军国民警卫队增强型网络训练模拟器靶场等。在靶场联合试验训练方面,美军已经进行了实践,如联合网络空间作战靶场于2012年夏与美国国家网络靶场进行了集成,据称,集成达到了前所未有的程度。美军声称,美军能够通过不同的连接方法或集成方法,将这些靶场进行连接或集成。

值得一提的是,美国诺思罗普·格鲁曼公司位于马里兰州米勒斯维尔的网络靶场不仅与美国国内的多个网络靶场、试验中心、研究中心相连,还与公司负责承建的英国网络靶场、澳大利亚网络靶场等相连。

##### 3. 大量采用新技术和仿真技术

在网络靶场建设中,美军大量采用了新技术,使这些靶场既可独立承担试验训练任务,又可联合开展试验训练任务;既可以并行进行试验训练,又可以串行进行试验训练;既可以开展非密级的试验训练,又可以开展带密级的试验训练。而且,靶场可以在极短的时间内完成配置、复位和重新配置等。另外,网络靶场不与现实中的任何网络连接,完全在封闭的网络环境中运行。据参与国家网络靶场第一阶段建设的诺思罗普·格鲁曼公司称,在2009年前,公司在网络靶场的建设中主要专注于物理仿真,但在后来为英国和澳大利亚建设网络靶场中,则采用了虚拟技术。

为了逼真地模拟各种网络,靶场非常注重提高网络模拟器的保真度和逼真度。美军认为,网络模拟器无风险的环境和基于情景的激励可以让作战人员:体验和进行包括破坏、阻断网络的完整性等活动;渗透到模拟的计算机网络中进行情报搜集;对防御和保护网络的程序和战术进行训练;等等。美军网络模拟器的开发始于2000年左右,如美国空军于

2001 年便开始了网络模拟器的开发建设。据报道，目前美国在用的网络模拟器已达 100 多个，而且随着时间的推移和技术的不断发展，美军对网络模拟器的需求也在发生变化，网络模拟器的功能也在不断提高。网络模拟器已从过去仅仅是复现、模拟蓝军的日常作战环境发展为能够模拟“红军”的威胁环境，而且还涵盖了“灰色”威胁环境（所谓“灰色”威胁，系指采用了西方技术加以改进的“红军”威胁）。

#### 4. 坚持遵循军民融合式发展道路

军民融合是指将国防科技工业基础与更大的民用科技工业基础结合起来，组成一个统一的国家科技工业基础的过程。美国一直扮演着军民融合理论与实践探索者的角色。多年来，美国通过军民两用技术发展计划，使之始终保持军事技术上的领先地位。在网络靶场建设、软件工具开发和网络作战人员培训方面，这点表现得尤为突出。

众所周知，美国国防工业巨头技术实力非常雄厚，在网络技术方面亦是如此。洛克希德·马丁公司和诺思罗普·格鲁曼公司这两个国防工业巨头都建立了自己的网络靶场，并且分别是美国国家网络靶场和英国网络靶场、澳大利亚网络靶场的主承包商。凭借这些美国国防工业巨头的雄厚技术实力以及领先世界的 IT 技术，美军将网络靶场建设任务承包给了其国防工业巨头和 IT 公司，如在靶场建设方面，选定洛克希德·马丁公司为国家网络靶场主承包商，并由其负责靶场的运行和维护；在网络靶场模拟器以及软件和工具开发方面，大量选用了 IT 公司开发的产品，如国防部信息确保靶场采用了 Breaking Point 公司、Arc Sight 公司、Sourcefire 公司等开发的工具；在人员培训方面，雷锡恩公司等开发了用于军事人员进行网络训练的高逼真仿真软件工具，将逼真的网络空间作战场景整合到真实—虚拟—构造环境中。



# 第 5 章

## 网络空间作战态势感知

网络空间作战态势感知是近几年发展起来的一个热门研究领域，是一种有效的事前防御措施。它在融合各种网络空间作战要素的基础上从宏观的角度对网络空间作战环境信息进行收集，并对系统可能存在的威胁进行分析，以实现安全风险实时监测、精准预警和应急响应，对网络空间作战态势进行全面感知，为网络空间作战指挥人员的决策分析提供依据，将不安全因素带来的风险和损失降到最低。

### 5.1 基本概念与知识

#### ■ 5.1.1 网络空间态势感知的内涵

##### 1. 态势

态势（situation）这一理念源于军事战争领域，通常用在刻画一个较大范围的、环境动态变化的、受多因素影响的、内部结构比较复杂的被研究对象的整体的状态和变化的趋势。随着计算机技术和通信技术的快速发展，大规模网络也逐渐呈现出上述状态和变化的

趋势。参照现代汉语词典可知，态势即是一种状态和趋势，是一个整体和全局的概念，任何单一的情况或状态都不能称之为态势。从本质上来说，态势就是相关时间和空间事实的集合，这些事实由目标间的关系组成。图 5-1 描述了组成态势的基本元素，包括环境、实体（存在）、事件（发生）、组和行动等五方面。在一定环境中存在的某事物即实体，当其性质或状态发生变化时，就产生了事件。而每个实体所发生的事件在时间和空间上都存在着某种联系，多个实体和事件按照某种关系组合在一起作为一个单位，就构成了组的概念。在特定环境中，成组或单个实体将会产生某种行动，而态势就是用来描述这一过程的。显然，态势的两个最活跃的元素是实体和事件。在实际应用中，为了完成态势感知，首先必须确定态势元素，而不同的应用环境，其态势元素的具体内涵可以各不相同，但是其基本构成成分不会改变。

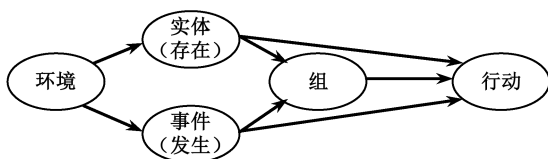


图 5-1 态势所包含的元素

网络态势指的是由于网络设备运行状况、网络行为以及用户行为等因素所构成的整个网络当前状态和变化趋势。网络态势从应用所关注的角度不同以及考察的应用层次不同，可以分为多种不同的态势，如网络的运行态势、可生存性态势、威胁态势、抗打击态势，以及从应用角度来看的舆情态势等。

需要特别注意的是：

(1) 态势的概念是面向“环境”而言的。网络态势的应用环境是在一个较大的范围内具有一定规模的网络。

(2) 态势强调动态性。态势信息不仅包括当前的状态，还要对未来的趋势做出预测，这些预测有些是根据历史数据做出的不太确定的推测，有些是根据一些先兆信息做出的比较确定的判断。

(3) 态势强调整体性。态势是各实体间相互关系的体现，某些网络实体状态发生变化，会影响到其他网络实体的状态进而影响整个网络的态势。

## 2. 感知

感知(awareness)通常是指客观事物通过感觉器官和感应器件在人脑中或系统中的直接反映。主体不仅能观测对象，而且能从所观测的现象中得出结论。感知包含着感官知觉和直觉，比如面对一个陌生人，有的人能感知到他心里想什么，有的人只能感知到他长什么样，前者是直觉，后者是感官知觉。

机器感知是指用机器或计算机模拟、延伸和扩展人的感知或认知能力，包括机器视觉、机器听觉、机器触觉……如计算机视觉、模式识别、自然语言理解等方面。

网络感知技术能够感知底层物理网络的状态，根据感知结果指导层叠网的拓扑构建，

优化层叠网应用产生的网络流量,缓减骨干网压力,是解决层叠网带宽浪费问题的一个重要途径。

感知网络是指通信网络能够感知现存的网络环境,通过对所处环境的理解,实时调查通信网络的配置,智能地适应专业环境的变化。

感知网是一个视频监控即服务架构的远程视频监控服务平台,通过互联网实现网络视频监控设备的接入,给用户的安全便利的远程访问、智能分析、联网告警等全方位的服务。越来越多的网络摄像机、网络视频服务器能够接入感知网,把用户从固定地点解放出来,利用碎片化的时间也能够享受视频监控带来的安心和便利。

### 3. 态势感知 (SA, Situation Awareness)

SA 这个概念首先出自军事领域,是对战场态势进行评估以获得决策支持的过程,常用于航天飞行中的人因研究、人机交互系统等,表现出极佳的实用价值后被广泛应用在航空管制、军事战场、核反应堆控制和医疗应急调度等领域。

这个概念由前美国空军首席科学家 Endsley 在 1985 年进一步规范,给出了 SA 的定义,即“态势感知是在特定的时间和空间下,对环境中各元素或对象的觉察、理解以及对未来状态的预测”。

- (1) 觉察:检测和获取环境中的重要线索或元素,这是 SA 中较基础的一步;
- (2) 理解:整合觉察到的数据和信息,分析其相关性;
- (3) 预测:基于对环境信息的感知和理解,预测未来的发展趋势,这是 SA 中最高层次的要求。

美国学者 Dominguez 把 SA 的基本定义扩展为四个阶段:

- (1) 提取环境信息;
- (2) 整合当前环境的信息和相关的环境内部元素的信息,生成当前态势视图;
- (3) 利用当前的视图去指导更进一步的感知获取;
- (4) 对未来的事件进行预测。

把这个概念引入网络空间安全领域的是美国空军通信与信息中心的 Tim Bass,1999 年他提出了网络态势感知概念,将 SA 技术用于网络管理和网络空间安全领域,提高管理者对所保护网络的认知,目的在于缩短管理者决策的时间并提供相应决策辅助。Tim Bass 提出通过融合推理来识别攻击者的身份、攻击频率、攻击速度、攻击目标和攻击威胁性等,从而达到对当前网络的安全态势感知。Greg Cole 和 Natasha Bulashova 定义网络空间作战态势感知是网络管理者通过人机交互界面达到的对网络空间安全状况的认知,主要实现一定地理区域内网络流量信息的可视化,如世界区域、国家、城市、机构/组织、IP 域、网络协议及时间周期等信息。其生成的网络空间作战 SA 视图,可帮助网络管理人员直观地看到网络当前的安全状况,以便于作出安全决策。

针对指挥控制系统的核心环节,Endsley 在 1988 年国际人因工程 (Human Factor) 年会上提出了有关 SA 的一个共识概念,即在一定的时间和空间内对环境中的各组成成分的感知、理解,进而预知这些成分的随后变化状况。动态决策态势感知模型如图 5-2 所示。

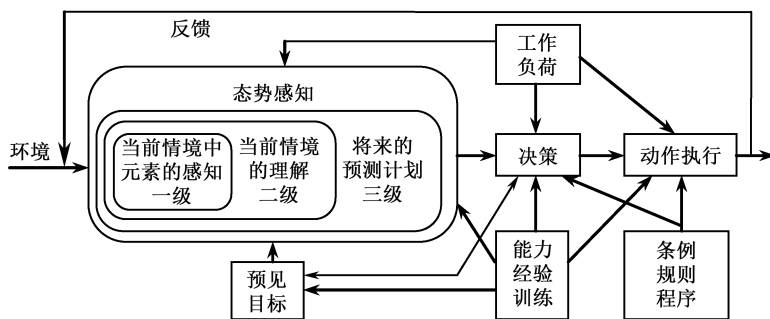


图 5-2 动态决策态势感知模型

从图 5-2 可以看出，根据预见目标、能力、经验、训练、工作负荷和动作执行，对外部环境进行 SA。该模型分成三级，每一阶段都是先于下一阶段，沿着一个信息处理链，从感知通过解释到预测规划，从低级到高级，具体为：第一级是对环境中各成分的感知（信息的输入），第二级是对目前的情境的综理解（信息的处理），第三级是对随后情境的预测和规划（信息的输出）。通过态势要素获取，获得必要的数据库；通过数据分析进行态势理解，进而实现对未来短期时间内的态势预测。随后提出决策，且预测执行信息，最终通过整体或全局的控制方式，保障网络运行环境安全性。但在 SA 决策过程中，个人因素和系统因素将影响 SA 效果，其中，个人因素包含预见、目标、知识、能力、训练、经验等，而系统因素涵盖了工作压力、工作量、系统设计、复杂性等。通过定性或定量的态势评价体系对底层各类事件进行归并、关联和融合处理，并将获取的 SA 结果以可视化图形提供给工作人员。

SA 是反映趋势的，是动态的、可预测的，所以它需要更多的事件、更多的情报，以及很多很多的历史数据才可以完成的。SA 需要通过大局来跟踪和决策。

SA 的研究重点在于各种复杂信息的高效组织和可视化应用。其目的就是抽象的数据组织、表征为人能够理解的图表、统计数据等，使指挥官了解双方的情况，包括敌我所在位置、当前状态和作战能力，以便能做出快速而正确的决策，达到知己知彼、百战不殆的目的。

#### 4. 网络空间态势感知（CSA, Cyberspace Situation Awareness）

CSA 是对网络系统作战状态的认知过程，是通过多传感器多手段协同侦察的方式，通过入侵检测、显示、精炼、过滤和融合等方法，对能够引起网络空间态势发生变化的所有环境要素进行获取、理解和评估，并预测其发展趋势，以便网络空间作战人员对网络空间内的安全要素、安全设备、信息系统进行合理的调整、升级，应对网络空间作战态势的变化，最终取得作战主动权。具体包括以下五个方面：

（1）收集网络中能够收集到的信息，主要是网络安全设备的报警记录、网络链接设备产生的流量记录、用户行为信息、网络进攻信息、网络漏洞信息及网络空间中所有电子设备和电子系统的运行状况等。

(2) 对各种影响系统安全性的要素进行检测获取, 觉察网络当前发生的安全事件, 安全要素包括电磁信号层、通信与网络协议层、信息层和行为层的安全信息。

(3) 对采集到的多源安全信息采用分类、归并、关联分析等手段进行融合, 得到规范化的数据。

(4) 对融合的数据进行综合分析, 搜集有用的信息, 实现对系统的背景状态及活动语义的提取, 分析当前网络所遭受的攻击状态, 识别出存在的各类网络活动以及其中异常活动的意图, 从而获得据此表征的网络空间作战态势和该态势对网络系统正常行为影响的了解, 评估网络空间的安全态势, 并给出相应的应对措施。

(5) 对网络空间的安全态势的发展趋势进行预测, 及时预警, 从而提早地进行响应, 预防大规模安全事件的发生, 减轻网络敌方行动的危害。

基于大数据的网络空间作战态势感知, 通过整合用户终端、网络链路、应用系统、数据流量等各类感知数据源, 利用大数据分析挖掘技术, 使用智能算法和安全模型, 将看似毫无联系、混乱无序的各类安全数据转化成直观的可视化信息, 实现威胁发现、精准预警和态势感知。

CSA 系统不仅包括硬件传感器(如网络接口卡)和智能计算机程序(如可以获悉攻击特征的程序), 还包括高级决策的人类思维过程。它依赖于入侵检测系统、日志文件传感器、反病毒系统、恶意软件检测程序以及防火墙等网络传感器, 这些传感器都生成比原始数据包更抽象的事件。

获取网络空间态势的方法目前包括漏洞分析(使用攻击图)、入侵检测与告警关联、攻击趋势分析、因果关系分析和取证分析(例如对入侵的反向追踪)、污点分析和信息流分析、损害评估(使用依存关联图)和入侵响应等。

随着对 CSA 研究的深入, 它从一个理论概念逐渐丰富为一套理论模型, 其中包括态势感知的数据分析方法、表征态势的指标体系、态势指标的呈现方式、安全态势感知的核心技术等。

### 5.1.2 态势感知技术分类

人们出于解决行业领域内具体问题这一目的, 从信息收集、感知方法及过程等角度研究态势感知。若从军事与国土安全决策支持及知识管理方面讨论问题, 可以从信息获取、存储、解释等角度分析态势感知。若从讨论网络空间作战态势感知方面来看, 可以从基于事件和环境角度来研究态势感知。下面不局限于某一具体的应用领域或角度, 而从更高层面对态势感知技术进行分类, 如图 5-3 所示, 以期更全面地探究态势感知技术。

#### 1. 环境类型

环境类型分为封闭式环境和开放式环境。封闭式环境或闭合系统, 指不与外界有任何

物质交换，不受任何外力控制或影响的系统。如一个核电厂的整个运行监控系统，其特点是观察对象固定，对象的特征与对象间关系稳定且可枚举，此类环境的态势感知相对容易。

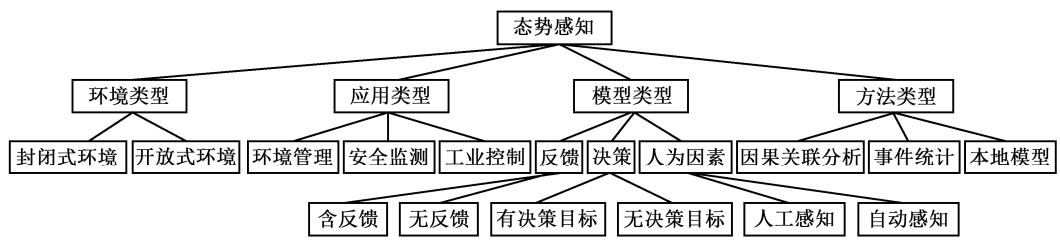


图 5-3 态势感知技术分类

开放式环境如战场、互联网等，其特点是环境中的对象类型、特征均可能发生变化，环境无边界或边界模糊。为了简化，这类环境的感知模型会将对象进行粗略的分类，从而使对象类型固定。信息时代，这类环境更为常见，由于环境复杂度高，对态势感知技术的需求也更为迫切。

2. 应用类型

应用类型主要有环境管理、安全监测和工业控制，不同类型间的区别在于感知的目的不同，而这主要体现在感知过程的不同。

环境管理，如观察某一区域的车辆通行情况，观察记录某地气象走势等。通过记录、统计、分析，为将来的设计提供决策等。

安全监测，这包括对环境中异常的检测，攻击的识别，威胁的评估，主要目的是宏观的安全管理。

工业控制包括对工业生产环境的过程控制，主要目的是确保工业生产活动的安全、质量、效率等。

以上应用类型的不同主要体现在态势感知过程的不同上，应用类型与态势感知过程见表 5-1。

表 5-1 应用类型与态势感知过程

应用类型	态势感知过程				
	环境信息收集	对象识别	基于感知模型的态势感知	异常监测及告警	反馈
环境管理	√	√	√	—	—
安全监测	√	√	√	√	—
工业控制	√	—	√	√	√

3. 模型类型

模型类型可以根据有无反馈、有无决策目标、有无人为因素来划分。需要注意，有时这些因素之间是相关的，如有决策目标的模型，为了提高模型的准确度，往往需要通过评

估决策的效果并通过反馈修正模型；而具有多元决策目标的评估模型，由于决策过程的复杂性，往往需要加入人为干涉来调整感知模型。

除此以外，模型类型还可以基于数据源（单一、多源、多源异构）、模型特点（基础模型、融合模型、领域模型）、所用方法（概率统计、关联分析）等特征。

4. 方法类型

方法类型主要有因果关联分析、事件统计和本体模型三类。

因果关联分析是通过分析环境中发生事件的因果关系，来理解、确定或预测环境的状态。具体来说，环境信息通过基于因果关系的感知模型，映射为环境的状态，这类方法适用于环境中的对象及其行为之间存在因果关系的场合。

事件统计是指按照事件发生的统计结果来评估环境状态，这类技术通常需要使用基于训练数据的机器学习方法，学习的目标是建立特定事件模式与环境知识状态之间的映射关系，新的事件通过这种映射关系的映射形成对环境态势的感知，这类方法适用于具备质量较高的环境事件统计数据的情况。

本体模型是通过对环境本身时空特性的分析，归纳并推断当前及未来的态势。例如，通过分析一个网络中服务的漏洞情况来判断未来网络的安全态势，通过分析一个区域的安设设施维护情况来推断这个区域的安全风险等。

各种态势感知技术比较见表 5-2。

表 5-2 各种态势感知技术比较

方法	技 术	优 点	缺 点
因果 关联 分析	贝叶斯推理	态势感知过程明确	需要态势感知模型及相关测度，开发成本高
	模糊推理	基于专家知识的推理规则，易于理解	隶属函数及推理规则的调整工作量较大
	模糊认知图	态势感知级别更高，决策转换方便	需要高质量专家知识
事件 统计	机器学习、神经网络	分类规则、易于理解	需要高质量训练数据及专家知识
	隐式马尔科夫链	可以融合异质传感器信息， 进行三级态势感知	需要高质量训练数据
本体 模型	状态图模型	语义清晰、易于实现	仅适用于状态、转换比较简单的场合

5.1.3 网络空间作战态势感知的目的、原则与任务

1. 目的

网络空间作战态势感知的目的是对网络态势状况进行实时监控，对潜在的、恶意的网络行为变得无法控制之前进行识别、防御、响应和预警，给出相应的应对策略，将态势感

知的成熟理论和技术应用于网络空间作战和安全管理；在急剧动态变化的复杂网络环境中，高效组织各种安全信息，宏观把握整个网络的安全状态，将已有的表示网络局部特征的指标综合化，使其能够表示网络空间安全的宏观、整体状态，从而加强指战员对网络空间作战的理解能力，为高层指挥人员提供决策支持。

就较高层次而言，网络空间态势感知综合研究的基本目标包括：

(1) 在机器具备足够人工智能前信息系统需由掌握全面网络空间态势感知的人提供保护。

(2) 开发新的算法，以实现：①极大地提升机器智能获取自我态势感知的能力，使得有一天机器能够实现自我保护；②人类决策者态势感知认知过程的自动化。

(3) 受保护的系统可以认识和学习不断演变的态势，生成并推理态势响应计划和行动，对入侵做出自动响应。

## 2. 原则

原则 1：网络空间作战的全面态势感知需要整体论方法，以集成感知、理解和预测。

原则 2：具备全面态势感知的信息系统必须有能力处理不确定性（如通过假设和推理）。

原则 3：网络空间作战态势感知必须在多个抽象层次获得。

原则 4：网络空间作战态势感知有两个大体正交的视角：生命周期视角包含了网络空间态势感知过程各阶段的内在机理，而人类认知视角则包含在网络空间态势感知总体框架（或解决方案）中融入人为分析的理论和技术。为提高人类态势感知的自动化能力，人类必须对希望获得感知的重要活动建模或加以识别。

## 3. 任务

网络空间作战态势感知的主要任务包括以下内容：

(1) 当前状态感知。亦称态势觉察，包括态势识别和态势确认。态势识别是意识到有攻击正在发生。态势确认包括攻击类型、攻击源、攻击属性、攻击目标等的确认。态势识别不仅仅是入侵检测，入侵检测只是其中一个非常基本的内容。入侵检测系统既不能识别攻击也不能确认攻击，在进行识别或确认过程中仅能简单地判别事件的发生，还需进一步确认是否是进攻行为的一部分。

(2) 攻击影响感知。亦称影响评估，包括当前影响评估（即损害评估）和将来影响评估（如果攻击者继续攻击的话）两个部分。脆弱性分析是影响评估的一大方面，提供了己方的状态知识，促进将来影响的预测。漏洞分析在很大程度上也是影响评估的一个方面，可以使我们了解自身情况，并预测未来的影响。将来影响评估还涉及威胁评估。

(3) 态势演化感知。态势追踪是其重要组成部分。

(4) 行动者（敌手）行为感知。其重要组成部分是攻击趋势和意图分析，更关心行动者（敌手）的行为，而不是态势本身。

(5) 感知当前态势形成原因和过程。包括因果关系分析（通过事后追踪）和事后分析。

(6) 感知收集到的态势感知信息素材与质量，以及从这些信息项中得到的知识—智能—决策的质量（可信性）。质量度量包括可信性、完整性和新鲜性。



(7) 态势预测。预测敌手将来可能的行为和动作、可能采取的攻击路径,分析得出可能的态势。该部分需要对敌手意图、机会、能力和自身脆弱性有全面了解。对合理前景的推断也可视为威胁识别与威胁评估的内容。

## 5.2 网络空间作战态势感知的主要技术

所谓的网络空间作战态势感知技术是指针对网络空间作战环境的管理模式,它能够作战人员提供一个统一的网络空间作战信息管理平台,利用历史痕迹及其相关内容对网络空间进行多角度的综合监测,精准地进行情况判断,提供准确的状态走势图。主要通过其本身具备的入侵检测系统、网络漏洞评估系统、防火墙和流量监测工具等维护网络空间作战设备的安全,对网络空间作战进行实时监控,同时还可以对网络中有关作战数据进行相关的采集和存储、分析,找出对于网络空间作战造成威胁的根本原因,进行及时的控制和治理,进而更好地保证网络空间的安全,夺取网络空间攻防作战的主动权。

### 5.2.1 入侵检测技术

当网络系统本身不可避免地存在脆弱性,筑高墙的方法无法阻挡黑客进攻时,网络不可避免地存在安全入侵,如果能及时检测并消除入侵,就可以减轻网络的安全损害,提高网络的安全性,因此入侵检测技术作为网络空间作战的第二道防线变得尤为重要。

入侵检测指检测网络入侵的技术,是对入侵行为的察觉、感知。利用计算机分析技术对计算机网络中各种行为进行监测分析,对各节点的运行进行追踪,从而发现那些满足入侵定义的异常行为。方法包括收集计算机操作系统信息、计算机系统程序和应用程序的信息、计算机网络信息等。

入侵检测技术已有着三十多年的历史。1986年,美国人 Anderson 第一次提出入侵的概念,将入侵定义为未授权的访问、篡改信息。1987年,美国 Dorothy Denning 教授给出了第一个入侵检测模型。该模型主要根据主机系统审计记录数据,生成有关系统的若干轮廓,并监测轮廓的变化差异发现系统的入侵行为。早期的入侵检测模型如图 5-4 所示。

入侵检测技术分为两类:异常检测和误用检测。异常检测首先检测系统的正常行为,描绘系统的正常行为轮廓,然后给出一个阈值,并分析系统的当前行为,对比实时系统的轮廓值与阈值,

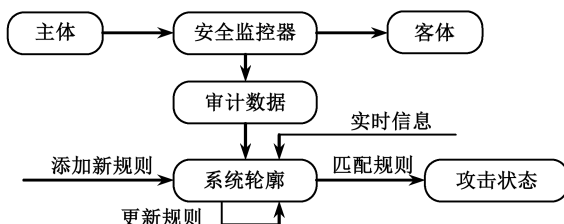


图 5-4 早期的入侵检测模型

从而判断是否有入侵事件的发生，如果有则做出响应，如警报、断网等。误用检测首先提取已知的进攻行为的特征，建立特征知识库，然后将检测到的系统行为与知识库中的进攻行为特征进行比较，如果发现能够匹配，进而判断系统有入侵发生。异常检测技术与系统无关，通用性强，对未知攻击有一定的检测能力，但是该技术需要很多的主机正常行为作为先验知识，而准确全面定义主机的正常行为轮廓非常困难，因此异常检测的误报率很高。误用检测技术原理简单，易于扩充，但是只能检测已经存在的进攻行为，警报正确率较高，但是漏报率也较高，对于未知的入侵行为或变异的入侵行为却无能为力。

目前，有多种对网络空间进行入侵检测的方法，常见的主要有以下几种。

### 1. 统计方法

统计方法是产品化的入侵检测系统中常用的方法，它通常用于异常检测。基于特征选择的异常检测方法，系指从一组度量中选择能够检测出入侵的度量、构成子集，从而预测或分类入侵行为。统计方法是一种较成熟的入侵检测方法，它使得入侵检测系统能够学习主体的日常行为，将那些与正常活动之间存在较大统计偏差的活动标志为异常活动。

### 2. 专家系统

该技术根据安全专家对可疑行为的分析经验来形成一套推理规则，然后在此基础上建立相应的专家系统，由此专家系统自动进行对所涉及的入侵行为进行分析。该系统可以随着经验的积累而不断自我学习，并进行规则的扩充和修正。

用专家系统对入侵进行检测，经常针对有特征的入侵行为。专家系统的建立依赖于知识库的完备性，知识库的完备性又取决于审计记录的完备性与实时性。

### 3. 基于模型的入侵检测方法

入侵者在攻击一个系统时往往采用一定的行为序列，如猜测口令的行为序列，这种行为序列构成了具有一定行为特征的模型，根据这种模型所代表的攻击意图的行为特征，可以实时地检测出恶意的攻击企图。与专家系统通常放弃处理那些不确定的中间结论的缺点相比，这一方法的优点在于它基于完善的不确定性推理数学理论。基于模型的入侵检测方法可以仅监测一些主要的审计事件，当这些事件发生后，再开始记录详细的审计，从而减少审计事件处理负荷。

### 4. 模式匹配

模式匹配是将收集的信息与已知的网络入侵和系统已有模式数据库进行比较，从而发现违背安全策略的行为。该过程可以很简单（如通过字符串匹配以寻找一个简单的条目或指令），也可以很复杂（如利用正规的数学表达式来表示安全状态的变化）。一般来讲，一种进攻模式可以用一个过程（如执行一条指令）或一个输出（如获得权限）来表示。该方法的一大优点是只需收集相关的数据集合，显著减少系统负担，且技术已相当成熟。它与病毒防火墙采用的方法一样，检测准确率和效率都相当高。但是，该方法存在的弱点是需要不断地升级以对付不断出现的黑客攻击手法，不能检测到从未出现过的黑客攻击手段。

## 5. 状态转移分析

状态转移分析主要使用状态转移表来表示和检测入侵。入侵行为是由攻击者进行的一系列操作,这些操作可以让系统从某些初始状态迁移到一个危害系统安全的状态,每次转移都是由一个断言确定的状态经某个事件触发转移到下一状态。在状态转移分析中,入侵检测被表示成为目标系统的状态转换图。当分析审计事件时,若根据对应的条件布尔表达式,系统从安全状态转移到不安全状态,则该事件标记为入侵事件,其中对应的条件布尔表达式能够表示已知的入侵特征。

## 6. 神经网络

这种方法利用神经网络技术来进行入侵检测。神经网络具有自学习、自适应的能力,通过接受训练,不断地获取并积累知识,进而具有一定的判断和预测能力。只要提供系统的审计数据,神经网络就会通过自学习从中提取正常的用户或系统活动的特征模式。神经网络优点在于避开了选择统计特征的困难问题。

## 7. 规划识别

入侵检测系统不仅能识别已经攻击过的行为和正在进行攻击的行为,而且还必须能从分析黑客的行动中推测下一步的规划,同时对即将实施的行动进行预警和响应。在人工智能领域中,从观察到的动作或状态推测未来动作或状态的规划称为规划识别。通过在入侵检测系统中采用规划识别方法,就可以预测黑客的下一步行为,并提前采取措施来避免入侵或破坏的发生。

## 8. 遗传算法

遗传算法抽象于生物体的进化过程,是基于自然选择中适者生存、优胜劣汰原理而建立的,用于解决最优化的搜索算法。

将遗传算法用于入侵检测,主要是因为基于遗传算法的入侵检测系统是一种基于自我学习的入侵检测系统,它可以模拟自然进化的过程,使特征库中的初始特征值进化发展,动态更新入侵检测特征库,从而得到针对特定检测环境的最优特征集合。

## 9. 人工免疫系统

人工免疫系统是从生物免疫系统的运行机制中模仿而来的,它借鉴了一些生物免疫系统的功能、原理和模型。

生物学中的免疫系统可以通过对自我和非自我的识别达到清除非自我细胞的能力,入侵检测系统中的入侵检测与免疫系统发现非自我的识别能力非常相似,因此,可以将生物学中的免疫判断机制引入到网络入侵检测中。

## 10. 其他新技术

随着网络及其安全技术的飞速发展,一些新的入侵检测技术相继出现,主要包括软计算方法、移动代理、数据挖掘、协议分析及命令解析技术等。

上述攻击检测方法和技术单独使用并不能保证准确地检测出变化无穷的入侵行为。在网络安全防护中应该充分权衡各种方法的利弊，综合运用这些方法，才能更为有效地检测出入侵者的非法行为。

## 5.2.2 信息融合技术

信息融合技术也称为数据融合技术，或者多传感器数据融合。它是把来自不同数据源的数据进行结合的方法；是一种利用计算机技术，对来自多种信息源的多个传感器观测的信息，在一定准则下进行自动分析、综合，以获得单个或单类信息源所无法获得的有价值的综合信息，并最终完成其任务目标的信息处理技术。

成立于 1986 年的美国三军政府组织实验室理事联合会（JDL, Joint Directorate of Laboratories）从军事应用的角度将信息融合定义为这样一个过程：把来自许多传感器和信息源的数据和信息加以联合、相关和组合，以获得精确的位置估计和身份估计，以及对战场情况和威胁及其重要程度进行适当的完整评价。Waltz 和 Llinas 对上述定义进行了补充和修改，给出了如下定义：信息融合是一种多层次、多方面的处理过程，这个过程是对多源数据进行检测、互联、相关、估计和组合以达到精确的状态估计和身份识别，以及完整的态势评估和威胁评估。

就信息融合的标准而言，美国数据融合专家组成立之初就进行了相应的工作，且创建了数据融合过程的通用模型，也就是 JDL 数据融合处理模型，如图 5-5 所示。该模型是目前数据融合领域基于功能的经典的融合概念模型，其目的希望在多个应用领域都能通用。这个模型主要有四个关于数据融合处理的过程，即目标提取、态势提取、威胁提取和过程提取。这些过程在划分上并不是根据事件的处理流程，每个过程也并没有规定的处理顺序，实际应用的时候，这些过程通常处于并行处理的状态。该模型各层级的具体含义如下：

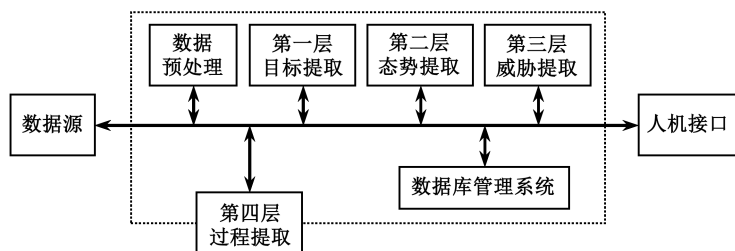


图 5-5 JDL 数据融合处理模型

### 1) 目标提取

利用各种观测设备，对不同的观测数据进行收集，然后把这些数据联合在一起作为描述目标的信息，从而产生目标的轨迹，进而形成目标趋势，同时显示该目标的各种属性，

如类型、位置和状态等。

#### 2) 态势提取

根据感知态势图的结果将目标进行联系,进而形成态势评估,或者将目标评估进行联系。

#### 3) 威胁提取

根据态势评估的结果,对有可能存在的威胁建立威胁评估,或者将这些结果与已有的威胁进行联系。

#### 4) 过程提取

明确怎样增强上述信息融合过程的评估能力,以及怎样利用传感器的控制获得最重要的数据,最后得出最大限度提高网络空间安全评估的能力。

信息融合所采用的主要技术有:(1)经典的推理和统计方法;(2)贝叶斯推理技术;(3) Dempster-Shafer 证据理论;(4)聚类分析;(5)熵法;(6)品质因数(FOM)技术;(7)专家系统和人工智能技术;(8)神经网络技术等。

信息融合技术为研究者建立下一代的网络管理系统或入侵检测系统,进而获取网络空间作战态势感知提供了重要的功能性框架。

### 5.2.3 数据挖掘技术

#### 1. 基本概念

数据挖掘就是通过采用自动或半自动的手段,对数据进行一定的处理,从大量的、不完全的、有噪声的、模糊的、随机的实际应用数据中,发现和提取有意义的、隐含在其中的、人们事先不知道的但又是有效的、新颖的、潜在有用的、最终可被理解的信息和知识的过程。从另外一个方面来说,数据挖掘是从数据中自动地抽取模式、关联、变化、异常和有意义的结构。它可将信息和知识转换为概念、模式、规则、规律等形式。

与数据挖掘相近的同义词有知识提取、知识发现、数据融合、数据/模式分析、数据考古学、数据捕捞和信息收获等。它汇聚了数据库、人工智能、机器学习、统计学、可视化技术、神经网络、模糊/粗糙集理论、模式识别、图像分析、信号处理、高性能并行计算等不同学科和领域的知识。

#### 2. 分类

根据不同的标准,数据挖掘系统可以分类如下:

(1) 根据数据模型分类, 可以分为关系的、事务的、面向对象的、对象-关系的或数据仓库的数据挖掘系统。

(2) 根据所处理的数据的特定类型分类, 可以分为空间的、时间序列的、文本的或多媒体的数据挖掘系统。

(3) 根据数据挖掘的功能, 可以分为特征、区分、关联、聚类、局外者、趋势和演化分析、偏差分析、类似性分析等数据挖掘系统。

(4) 根据所挖掘的知识的粒度或抽象层进行区分, 包括泛化知识(在高抽象层)、原始层知识(在原始数据层)或多层知识(考虑若干抽象层)。

(5) 根据所用的技术分类, 这些技术可以根据用户交互程度(如自动系统、交互探查系统、查询驱动系统), 或所用的数据分析方法(如面向数据库或数据仓库的技术、机器学习、统计、可视化、模式识别、神经网络等)描述。

(6) 根据挖掘任务可以分为分类或预测模型发现、数据总结与聚类发现、关联规则发现、序列模式发现、相似模式发现、混沌模式发现、依赖关系或依赖模型发现、异常和趋势发现等。

(7) 根据挖掘对象可以分为关系型数据库挖掘、面向对象数据库挖掘、空间数据库挖掘、时态数据库挖掘、文本数据源挖掘、多媒体数据库挖掘、异质数据库挖掘、遗产数据库挖掘、Web 数据库挖掘。

### 3. 主要功能

数据挖掘主要有以下五种功能:

(1) 自动预测趋势和行为。自动在大型数据库中寻找预测性信息。

(2) 关联分析。若两个或多个变量的取值之间存在某种规律性, 就称为关联。其目的是找出数据库中隐藏的关联和数据之间的规律性。

(3) 聚类。将物理或抽象对象的集合分成由类似的对象组成的多个类的过程被称为聚类。

(4) 概念描述。概念描述就是对某类对象的内涵进行描述, 并概括这类对象有关特征。

(5) 偏差检测。偏差包括很多潜在的知识, 如分类中的反常实例、不满足规则的特例、观测结果与模型预测值的偏差、量值随时间的变化等。

### 4. 数据挖掘的方法、语言和工具

数据挖掘的方法主要有分析和预测方法、粗糙集理论、模糊集合论、聚类分析、关联规则法、决策树法、人工神经网络、多媒体数据挖掘、数据可视化、遗传算法、近邻算法、联机分析处理和多层次数据概化归纳等方法。

数据挖掘语言主要有三种类型: 数据挖掘查询语言(DMQL), 典型代表有基于结构化查询语言的多媒体查询语言(MSQL); 数据挖掘建模语言, 典型代表有预言模型标记语言(PMML); 通用数据挖掘语言, 典型代表有微软推出的 OLE DB for DM 挖掘语言。

数据挖掘工具可以用来辅助技术人员进行数据挖掘的分析、设计和开发, 帮助用户快

速完成知识发现不同阶段的处理工作。数据挖掘工具根据其适用的范围分为两类：专用数据挖掘工具和通用数据挖掘工具。数据挖掘工具有以下几种：QUEST、MineSet、DBMiner、Intelligent Miner、SAS Enterprise Miner、SPSS Clementine、LEVEL5 Quest、Partek、SE-Learn、SPSS 的数据挖掘软件 Snob、Ashraf Azmy 的 SuperQuery、WINROSA、XmdvTool 等。

## 5. 数据挖掘的过程

数据挖掘的基本过程和主要步骤如图 5-6 所示，现在人们把数据挖掘作为知识发现中的一个过程来看待。

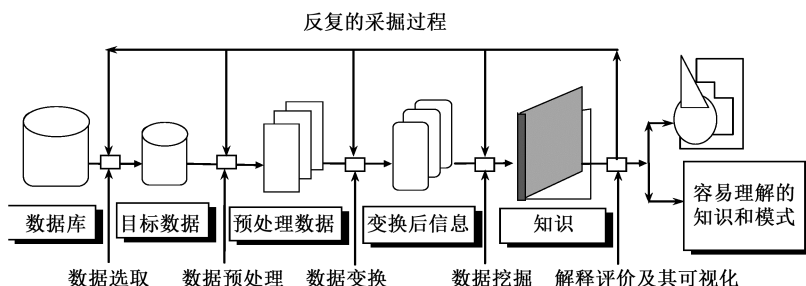


图 5-6 数据挖掘的基本过程和主要步骤

数据挖掘的过程包括以下几步：

- (1) 确定业务对象。清晰地定义出业务问题，认清数据挖掘的目的。
- (2) 数据准备。了解数据库中的知识发现应用的有关情况，包括熟悉相关的知识背景，搞清用户需求。
- (3) 数据选取。根据数据挖掘的目的和任务，确定操作对象，即目标数据；根据用户需要从原始数据库中选取相关数据或样本，利用一些数据库操作对数据库进行相关处理。
- (4) 数据预处理。数据预处理一般包括消除噪声或数据清洗，推导计算缺值数据，填充丢失数据，消除数据的不一致性，消除重复记录以及完成数据类型转换等。
- (5) 数据变换。数据变换的主要目的是消减数据维数或降维，或者对数据做一些相应的变换，通过投影或利用数据库的其他操作减少数据量。
- (6) 数据挖掘。确定数据挖掘要完成的功能和要发现的知识类型，选择使用什么样的挖掘算法。算法确定之后，由挖掘系统对数据进行分析，实现自动挖掘，从数据库中提取用户感兴趣的知识，并以一定的方式表示出来。
- (7) 结果的评价解释与可视化。对在数据挖掘步骤中发现的模式（知识）进行解释，并以可视化的形式输出，以便能够理解所获得的知识。通过机器评估剔除冗余或无关模式，若模式不满足，再返回到前面某些处理步骤中反复提取。
- (8) 知识同化。知识同化就是将前面数据挖掘所得到的知识集成到业务信息系统的组织结构中去，让其在信息系统中应用并得到检验，以确信本次发现的知识不会与以前发现的知识相抵触，并将发现的知识以用户能了解的方式呈现给用户。

## 6. 数据挖掘的逻辑模型

数据挖掘系统由一组构件联合组成，数据挖掘的逻辑模型如图 5-7 所示。

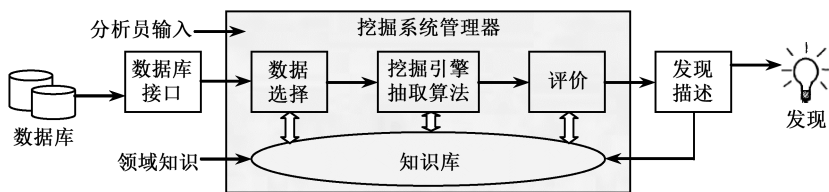


图 5-7 数据挖掘的逻辑模型

挖掘系统中的输入是数据库（或数据仓库）的数据、信息分析员的指导，以及存储在挖掘系统知识库中的知识和规则。选择的数据在引擎中处理，以生成辅助模式和关系。然后进行评价，通过与分析员交互以期发现令人感兴趣的模式。有些发现还要加入知识库中，以便后继的抽取和进行评价。

## 7. 数据挖掘在网络空间作战中的应用

### 1) 应用于网络安全入侵检测

(1) 应用的工作原理。将数据挖掘技术和网络入侵检测巧妙地结合在一起，在海量数据中挖掘审计数据，分析其特征性，从而找到异常数据对应的入侵行为。通过分析相应记录搜索出被攻击的特征性，利用数据挖掘技术可以更高效地找到入侵突破口，从而做出应对措施。

(2) 应用的技术优势。数据挖掘突出的优势体现在以下几点：①对数据的准确全面分析可以在数据挖掘环节中完美表现；②在数据发掘的关联规则基础上，巧妙结合算法分类、序列模型，让入侵检测更加高效准确；③在检测系统中应用数据发掘，不仅可以让搜索入侵口变得高效简单，而且这种新型思维有利于扩宽思路和弥补不足。思维的发散，让检测方式不再单一，不仅可以进行网络、主机的异常检测，还可以分组交叉进行。

### 2) 用于网络病毒防御体系

(1) 基本原理。如果蠕虫病毒感染计算机，先要扫描网络上的主机。以数据挖掘技术为基础，构建全新的网络病毒防御系统。该防御系统由数据源模块、预处理模块、数据挖掘模块、规则库模块、决策模块和防御模块等组成。其工作原理是：来自网络、发向本地的数据包形成数据源之后，由预处理模块处理，并且记录网络信息传输的病毒，以便对后期同等性质的病毒形成免疫力。一旦这些病毒再次非法入侵，系统就会及时警报，并且启动相应的保护防御程序。

(2) 具体应用方向。数据挖掘技术在计算机网络防御系统中的应用主要体现在以下几个方面：原始数据环节、数据分析处理环节、关联方式环节、数据挖掘环节、决策制定环节。



### 3) 在网络病毒防御体系构建中的应用

具体来讲,可以从以下几个角度探析其在计算机网络病毒防御过程中的应用:

(1) 数据源模块。该模块是以抓包程序为基础,截获网络向主机发送的数据包信息。数据源模块中有最原始的数据包和数据结构,在获取这样的数据源之后,要将其交给预处理模块进行下一步操作。

(2) 数据预处理模块。这是数据挖掘技术的基础性工作,这一工作会为后期数据分析打下良好的基础。它不仅关系数据挖掘成效,还涉及数据挖掘时间。

(3) 规则库模块。主要是存储检测到的病毒特征,并将其积累起来形成规则集。这一点反映出了病毒的特点和连接数据的规则,为后期病毒数据特点分析和收集提供相应的依据。

(4) 数据挖掘模块。借助科学的算法分析事件库,并且在此基础上生成请求记录,完成此项工作后将其交给决策模块。

(5) 决策模块。此模块分析数据挖掘的结果和规则库规则的匹配度。若发现两者之间的匹配度比较高,则说明数据包中可能有病毒;如果发现两者之间的匹配度很低,则可以在此基础上发动预警机制,找到新的蠕虫病毒,并将其纳入规则库中,实现规则库的扩展。

### 4) 数据挖掘技术下的病毒防御

一般情况下,主要通过以下几种分析方式进行病毒防御:

(1) 分类分析。简单来讲,就是将各个主体提前设定到几种类别中,以统计方法或机械方法建立分类模型,并在数据库实现特定类的数据映射,由此实现分类处理和分析。

(2) 聚类分析。它是指分解得到的数据包,将其归纳总结到不一样的组别中,而处于同组别中的往往都是有着彼此的相似点,不同组别代表不同特点的事物。以聚类分析的方式处理数据,可找到数据分布的疏密情况,并在此基础上形成全局的分布模式,进而展现数据之间的关系。

(3) 异类分析。异类分析又被称为孤立点分析,它是指分析数据库中明显偏离其他数据、明显具有不同点的数据,特指偏离了一般模式的数据。异类分析包括孤立点的发现和孤立点的分析,孤立点的发现常会产生有违常理的结果。在分析孤立点的过程中,则可能会发现比一般数据更有价值的数据。

(4) 序列分析。统计动态化的数据,研究随机数据序列归纳的情况,从而找到相应的病毒数据序列。一般情况下,序列分析的目的是最大限度地获取序列模式模型,来找到事件发生的时间序列。

### 5) 数据挖掘算法在网络安全审计中的应用

在安全审计中,运用数据挖掘技术,可以利用统计、分类、聚类、关联、序列分析、群集分析等方法,对网络日志中大量的数据进行深层次分析和研究,揭示其本来的特征和

它内在的联系，使它们转化为网络安全检测所需要的更直接、更有用的信息。

数据挖掘中的分类要解决的问题是为一个事件或对象归类。在使用上，既可以用它来分析已有的数据，也可以用它来预测未来的数据。安全审计可以看作是一个分类问题，希望能把每一个审计记录分类到可能的类别中，如正常或某种特定的入侵或操作异常。一般来讲，分类根据系统特征进行，关键就是选择正确的系统特征，大多数时候还需要根据经验和实验效果确定一个合理的阈值。

## 5.2.4 信息可视化技术

### 1. 概念与作用

信息可视化技术就是利用计算机图形学和图像处理技术，把数据信息变为图形或图像信息，使其能够以图形或图像的方式显示在屏幕上，同时利用交互式技术实现网络信息的处理。在目前信息可视化研究的领域不再局限于科学计算数据的研究，工程数据以及测量数据同样也实现了信息的可视化。利用信息可视化技术，可以有效地得知隐藏在数据信息中的规律，使网络信息的处理能获得可靠的依据。

网络空间作战态势感知体系的主要作用就是通过融合和分类多源信息数据，使网络空间作战人员在进行决策和采取措施时能及时和找准切入点。这就需要将态势感知最后得出的结果用可视化的形式在计算机系统中显示出来，充分发挥人类视觉中感知和处理图像的优势，从而保证网络安全状态能得到有效地监控及预测。同时，可视化技术将态势感知的结果以人们便于认识的形式呈现出来，那么就需要考虑到态势信息的及时性和直观性，最后显示的形式不能太过复杂。

### 2. 原始数据信息可视化

根据系统的要求，需要可视化的原始数据包括网元信息、流量信息、报警信息、漏洞信息以及各子网的静态信息。

(1) 网元信息。子网中活动的主机及该主机的 IP 地址、开放端口和它所提供的服务等信息，子网中存活的主机总数、端口总量信息。

(2) 流量信息。数据包大小的分布、数据包大小的分布的变化率、数据流总量、流量变化率、协议的分布、数据流入量、流入量增长率、流入数据源 IP 分布、带宽使用率、访问主流安全网站的频率等流量信息。

(3) 报警信息。子网的安全事件、历史安全事件发生频率。

(4) 漏洞信息。子网的网络漏洞及子网内各主机的主机漏洞。

(5) 静态信息。子网静态配置的安全信息。

### 3. 可视化技术分类

根据是否包括物理数据,可视化技术粗略地分为两类:科学计算可视化和信息可视化。

#### 1) 科学计算可视化

数据是抽象的、难以理解的,在研究过程中,很难对其产生比较直观的概念,因此,可以通过可视化工具,利用计算机图形学技术,将实验的数值转化为视觉上较易接受的图形图像,这就是科学计算可视化。通过计算将大量抽象数据进行转换后,可以轻松地对数据关系特征进行处理,并能高效地从中进行聚类分析,以获得新的构架。通过科学计算可视化的转换,随时间和空间变化的现象或数值以图像的形式直观呈现出来,这对于研究和分析变化趋势,模拟和验证既有算法模型,有不可估量的帮助。

#### 2) 信息可视化

信息可视化的过程,是将数据信息形象化,将人类的感知综合化的过程。通过信息可视化技术,可以将数据信息转换为可以直观形象理解的图形或图像表达方式,从而为计算机用户提供更为快捷、有效的服务。在网络态势感知的研究中,主要偏向信息可视化。

在传统的直方图、折线图等简单的图表中,目前已经可以添加丰富的色彩、实时的动画,甚至拓展到三维或多维空间进行展示。这些都为可视化技术的应用提供了必要的前提条件,也为充分发挥可视化技术的优势提供了保障。

总体来说,科学计算可视化的重点在于真实、快速地显示原始数据;信息可视化则侧重于设计和选择合适的显示方式,方便快捷地表示复杂的数据信息及其相互间的关系。

### 4. 可视化方法与技术

对数据进行可视化是一个层层递进的过程,包括了数据转化、图像映射、视图变换三个部分。数据转化是把原始数据映射为数据表,将数据的相关性描述以关系表的形式存储起来;图像映射是把数据表转换为对应图像的结构,图像由空间中的属性进行标志;视图变换则是通过对坐标位置、缩放比例、图形着色等方面来创建能够可视化的视图。此外,用户与可视化系统的交互也是必不可少的,用户通过调控参数,完成对可视化过程的控制。对于低维度的数据,可以采用传统的可视化方法,包括直方图、折线图、饼图、锯齿图、分位数图、局部回归曲线图等形式。对于多维数据,一般采用降维的方法,将数据间多维关系简化为二维的关系,从而简化问题的处理。下面介绍几种主要的可视化方法与技术。

(1) 几何投影技术。目前关于几何投影,主要有包括散点矩阵技术、平行坐标可视化技术、圆坐标可视化技术、放射性可视化技术、探测性统计学(如主成分分析、因子分析、维度缩放)、格架图等。

(2) 分层技术。对于多维空间,可以采用分层的形式对其进行抽象处理。将每个层次作为一个子空间,将每个维转换为若干个箱,并将其组合成栅格图像。子图像的数目与箱

的数目有关，每个子图像都有对应的外部维，因此由维转换的箱决定了子图像的数目。在确定数目之后，子图像会进行分解。分解的过程是递归的，它会在对应的箱的基础上进行，分解操作一直持续到所有维全部处理完毕为止。

(3) 失真技术。利用失真技术，可以从高细节和低细节两个层面来显示不同类型的数据，高细节的内容较少，低细节的内容较多。失真技术不仅有全局的展示，也有对重要细节的集中展示，对于交互式的探测有很大的帮助。最重要的失真技术有：Fish-eye 视图、压缩失真技术 Lryperbolic browser 等。

(4) 交互技术。交互技术是将分析的过程引入可视化的步骤中，利用相关联数据的交互，动态地展现不同的实体，以及它们之间的关系，从而使可视化效果更生动，更有意义。交互式技术包括映射、投影、过滤、缩放、链接和刷洗。其中，链接技术可以把多种可视化结果连接起来，可以方便比较多个模型，在可视化方面综合应用不同模型。

(5) 协同技术。协同技术是将原始数据与对应模型的展示形式进行对比，通过分析处理前后的可视化结果，对模型的运行效果进行分析研究，并从中找到改良模型的途径和重点。

(6) 钻过技术。通过钻过技术，可以了解结果是由哪些原始数据计算得来的。当模型定好之后，钻过技术会对利用其进行计算的原始数据进行处理，将其与结果建立关联，当需要分析某部分结果的来源时，可以方便快捷地获取原始数据。比如，利用决策树，可以对其分支进行选择和钻过，从而使用户可以获取与构造该分支有关的信息，而忽略其他信息的干扰。

(7) 虚拟技术。虚拟技术是在计算机软硬件技术发展前提下诞生的，它主要将待可视化的信息放置在虚拟的环境中，使用户能够体验身临其境的感觉。虚拟可视化也可称为虚拟现实，能够结合人的认知能力，使人充分融入数据挖掘的过程中。

## 5. 态势感知可视化流程

态势可视化系统的功能是向用户展示系统对网络空间作战事件的具体处理结果，通过便于理解的图形，动态地将抽象的感知信息展示出来。首先，数据收集系统不断收集网络空间的 NetFlow 信息、IDS 信息、防火墙过滤信息和黑客攻击等信息；然后，系统对这些信息进行态势评估和预测；紧接着由可视化分析、视图控制和交互控制组成的态势分析可视化系统根据中间数据结构的内容，结合可视化显示区域的大小，计算出每个节点在图上的位置，同时根据证据—事件的对应，根据用户的需求，按照不同网络级别，动态显示出每个节点所对应的具体事件，将网络中的安全指标、态势评估，以及态势预测结果动态地展示在多维的界面中。最后，管理员执行图形图像的接收、干预和管控，从而完成推理过程的可视化显示。态势可视化数据流图如图 5-8 所示。

## 6. 态势可视化的图像生成

首先根据态势综合指数，在电子地图中对各地区进行分级显示；再根据可视化信息初始化模块生成的信息组织方式，对静态和动态指标信息、攻击行为信息、监控对象信息、网络环境信息转化成图形图像模式；最后管理员可采用对应的统计图形模式进行显示，对用户选择的指标信息或指数信息进行可视化，其图形生成模式流程图如图 5-9 所示。

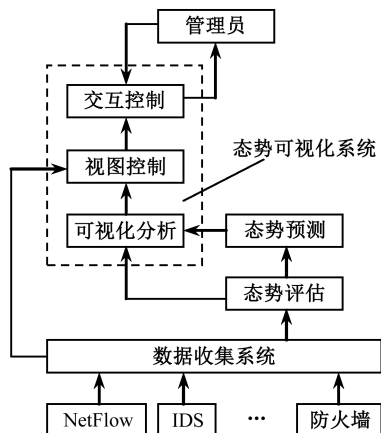


图 5-8 态势可视化数据流程图

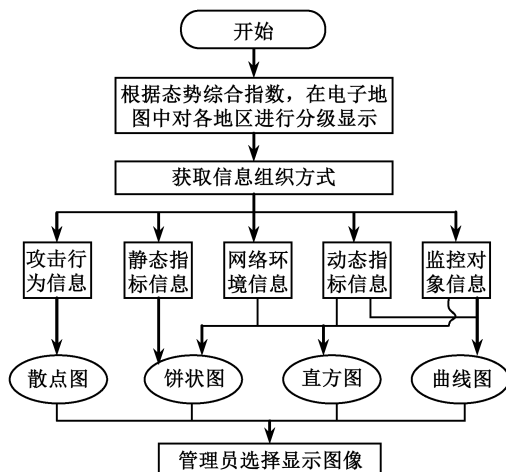


图 5-9 可视化图形生成模式流程图

### 5.2.5 恶意代码检测技术

恶意代码指对网络系统有恶意目的的程序，它危害系统运行，并能自行复制和传播。恶意代码从类型上分为病毒、蠕虫、特洛伊木马、后门、逻辑炸弹、间谍软件、僵尸网络客户端等。恶意代码一般利用系统的软硬件漏洞和欺骗用户的方式进行传播和破坏，如果系统中存在脆弱性而不存在利用该脆弱性的恶意代码，那么系统只是存在潜在的安全风险，并未出现安全损害，恶意代码是对系统造成安全损害的外因。恶意代码检测需要各种检测技术，识别出目标系统存在的恶意代码的特征和位置，包括基于特征码的静态检测技术、启发式扫描技术和基于虚拟机的行为检测技术。

基于特征码的静态分析技术是最基本、最常用的恶意代码检测技术，目前主流的防毒软件的查毒引擎大部分都采用这种技术。它首先对已存在的恶意代码样本进行分析，提取恶意代码的特征码，并写入相应的特征码库，然后对目标系统的文件进行扫描，若发现目标文件中有与特征码库相符的特征，则认为该文件含有恶意代码。基于特征码的检测技术具有实现简单、误报率低、查毒效率高的优点，但是检测结果依赖恶意代码的特征库，对已经存在的恶意代码能很好地检测，对未知、加壳变形和特征码难以描述的恶意代码不能

很好地检测，造成该技术存在大量的漏报现象。针对这种情况，目前的主流杀毒软件都提供实时的更新技术，及时更新病毒的特征库，并且采用广义特征码技术，能应对一些简单加壳和变形的恶意代码，但是在较为复杂的加壳加密的恶意代码面前，显得力不从心。

启发式扫描技术是对静态特征码扫描技术的一种改进，对恶意代码的特性进行分析，分析恶意代码指令出现的顺序和特定的指令组合，获得统计上的启发知识。在对文件扫描时，一旦发现目标文件中存在可疑的指令或指令组合，则认为目标文件含有恶意代码。该技术能够检测出未知的和变形后的恶意代码，但是在实现上非常复杂，尤其恶意代码的启发知识很难精确获取，因此误报率较高。

基于虚拟机的行为检测技术是在系统中虚拟 CPU 环境，在虚拟的环境中将恶意代码激活，根据其行为特征判断是否是恶意代码。该技术对未知的、加壳和变形后的恶意代码能有效地检测，并且不需要构建庞大的病毒特征库，能在一定程度上保证原系统的安全，因此该技术是目前杀毒软件的一个趋势。这种技术的检测模型如图 5-10 所示，主要包含两个部分：其一是深层检测与监控组件，负责检测和收集目标系统的各类信息，主要使用各种底层隐藏技术的恶意代码的行为信息；其二是基于行为分析的智能识别模块，包括行为知识库、知识获取组件和行为知识推理机，确保由检测信息有效识别恶意代码的行为。

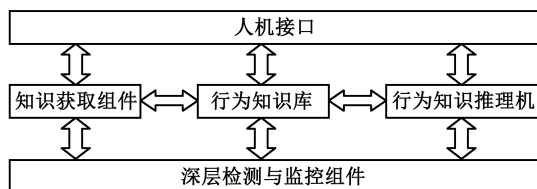


图 5-10 基于行为的恶意代码检测模型

但是基于虚拟机的行为检测技术存在两个缺点：其一是在系统中虚拟计算环境需要占用系统资源，对系统的性能产生影响；其二是激活恶意代码并分析其行为特征需要较长的时间，影响查毒效率。实现该技术难点是如何识别恶意代码的行为特征并构建行为特征库，需要确定哪些行为类型适合作为恶意代码的判断对象。

恶意代码检测技术对提高网络系统的安全性作用非常大，如果能有效地检测并及时清除系统中存在的恶意代码，可以减少系统受到的安全损害。但是恶意代码检测技术一般都是在系统存在恶意代码之后才能进行检测和清除的，此时恶意代码可能已经造成损害了，因此该技术并不能在第一时间阻止安全事件的发生，并且目前存在的恶意代码检测技术在检测的广度和精度上都不够，存在很多漏报和误报。因此，恶意代码检测技术对提高网络安全性作用有限。

## 5.2.6 风险分析与评估技术

网络系统中面临的风险是进攻或入侵发起者利用系统漏洞，导致信息资源损失的潜在

可能性。风险分析的重点建立在安全测评技术之上,就是确认网络系统中安全风险及其大小,确定风险等级和优先控制顺序的方法和工具,其以网络系统威胁、威胁所利用的漏洞以及潜在损失作为研究的出发点,对网络系统中的风险进行测量和分析。

当前研究阶段存在静态评估和动态评估两种风险评估技术。静态评估是指在攻击发生之前,主动地分析和评估被管系统中存在的风险和隐患,支持全面预防性的安全响应决策。动态评估是指在攻击发生之时,基于当前的安全警报进行实时评估和预判型评估,以支持有针对性的动态安全响应决策。目前这方面的研究内容多集中在损失评估方面,即分析相关攻击活动对被管网络已经造成的危害。

通常,根据描述方式的不同,分为定性的评估方法和定量的评估方法。其中,定性的评估方法是在风险评估过程中,仅使用定性的等级描述方式实现对评估因素的测量。定量的评估方法指对评估因素的测量通过数值体现,并且根据上述因素的测量值,利用一定的算法得到最终的风险值。在定量的风险评估过程中,评估步骤通常如下:

- (1) 确定关键资源及其价值,即确定所需要保护的对象,包括有形资源 and 无形资源。
- (2) 分析并量化资源所面临的威胁,分析可能对资源造成损失的潜在事件,并确定威胁可能发生的概率及潜在损失的大小。
- (3) 分析并量化系统脆弱点,即分析可能被威胁利用而造成损失的漏洞和安全隐患,并确定脆弱点可能被利用的概率。
- (4) 风险计算,即根据上述量化值,通过公式得到最终的量化风险值。

风险评估通常指的是在作战、生产和生活中人们对某一事件进行的量化评估。在发生风险事件或已经发生但并未结束的时候,人们为了了解该事件所造成或可能造成的影响,需要对该事件进行损失评价。

从网络空间作战和安全的角度看来,风险评估包括三方面内容,即威胁性评估、脆弱性评估和资源损失评估。进攻者利用计算机系统的漏洞或资源的薄弱点,对计算机进行进攻,从而造成用户资源的直接损失或潜在的损失。

风险评估是识别、评判、分析、检测和确定网络安全隐患风险的过程,是识别管理问题、制订管理策略服务的一项系统工作;是以威胁为出发点,结合系统脆弱性判断的评估过程;是周期性了解安全风险,采取相应安全控制措施的前提。它为降低网络风险、实施风险管理和控制提供了重要依据。风险评估是加强信息安全保障体系建设和管理的关键环节,是发现信息安全存在问题,找到解决方案的有效手段。

### 5.3 网络空间态势感知的主要手段

网络空间态势感知主要利用网络系统的协议特性、信息流特性、电磁特性和存储特性而对敌实施网络扫描、网络侦听、密码破译、介质窃密。

### 5.3.1 网络扫描技术及其算法

#### 1. 网络扫描的概念

网络扫描是根据对方服务所采用的协议，在一定时间内，通过自身系统对对方协议进行特定读取、猜想验证、恶意破坏，并将对方直接或间接的返回数据作为某指标的判断依据的一种行为。网络扫描的概念包含以下意思：

- (1) 网络扫描器几乎全部是客户端一方的程序，所针对的对象绝大多数是服务器方。
- (2) 网络扫描通常是主动的行为，绝大多数网络扫描器的扫描行为都是希望在服务器不知情的情况下偷偷进行，通常在扫描器的设计中，扫描行为应尽可能地避免被服务器察觉。所以扫描器通常不会对被扫描的主机有过多的要求，只能主动适应服务器的各项要求。
- (3) 网络扫描通常具有时限性。该时限虽然没有一个明确的界限，但一般来说都是接近扫描的最快速度。如果每隔几个小时访问一下某单位的网站主页，则不能算是扫描。
- (4) 扫描几乎都要用到工具，因为操作系统提供的程序并不都具有扫描的各项要求。
- (5) 扫描的目的通常是对预先的猜想进行验证，或者采集一些关心的数据。
- (6) 不可避免的一点就是，网络扫描更多地被黑客用于选择攻击目标和实施攻击，并且由于扫描自身的特点，通常被认为是网络进攻的第一步。

#### 2. 网络扫描的目的

网络扫描的目的一般是：

- (1) 获取某范围内的端口某未知属性的状态。这种情况下，一般不知道对方情况，只是想通过扫描进行查找。例如，通过扫描检测某个网段内都有哪些主机是开着的。
- (2) 获取某已知用户的特定属性的状态。这种情况下，一般都有明确的目标，有明确要做的事，接下来只是查找一下某些属性。如通过扫描检测指定的主机中哪些端口是开着的。
- (3) 采集数据。在明确扫描目的后，主动采集对方主机的信息，以便进行下一步的操作。如采集主机名、IP 地址、操作系统及版本号、提供的网络服务、用户名和拓扑结构等。
- (4) 验证属性。在明确扫描目标，并且知道对方具有某个属性的情况下，可以通过扫描验证自己的想法，然后判断下一步的操作。例如，通过扫描指定的服务，验证对方是否是 Windows 系列操作系统。
- (5) 发现漏洞。通过漏洞扫描，主动发现对方系统中存在的漏洞。如扫描对方是否具有弱密码。

#### 3. 网络扫描原理

根据扫描的概念可以发现，当一个主机向一个远端服务器的某个端口提出建立连接的请求时，如果对方有此项服务就会应答；如果对方未安装此项服务，即使向相应的端口发出请求，对方仍无应答。客户端向服务端发出请求的过程如图 5-11 所示。利用这个原理，



如果对所有熟知端口或自己选定的某个范围内的熟知端口分别建立连接，并记录下远端服务器所给予的应答，通过查看记录就可以知道目标服务器上安装了哪些服务，这个过程就叫作端口扫描，所使用的程序叫作扫描程序。通过端口扫描可以收集到很多关于目标主机的很有参考价值的信息，例如，对方是否提供 FTP 服务、万维网（WWW，World Wide Web）服务或其他服务。

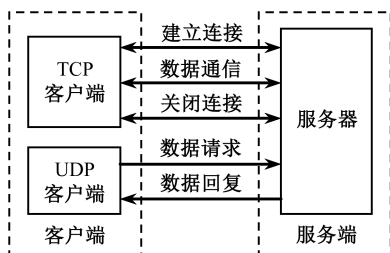


图 5-11 网络 TCP/UDP 扫描示意图

#### 4. 网络扫描技术

网络扫描技术大体分为四类：一是扫描目标，发现目标存活技术；二是收集系统相关信息技术，包括操作系统类型、所开放的服务等；三是根据收集的信息判断目标系统是否存在漏洞，或者进行模拟攻击检测；四是通过扫描等手段对指定的远程或本地计算机系统的安全脆弱性进行检测，发现可利用漏洞的一种安全检测（渗透攻击）行为。

第一类目标发现技术也被称为 Ping 扫描，其目的是为了发现目标主机或网络是否存活，采用的主要方法就是通过发送各种类型的内部控制信息协议（ICMP，Internal Control Message Protocol），或者 TCP、UDP 请求报文，通过报文发送结果判断目标是否存活。几种主要的方式包括 ICMP 广播、ICMP 扫描、ICMP 非回显、TCP 和 UDP 扫描。

第二类技术主要有目标信息收集技术。在确定有哪些目标存活的基础上，就要进行目标信息的收集工作，这其中包括目标主机的端口开放信息、操作系统类型信息以及开放的服务。所利用的技术主要有端口扫描技术、操作系统判别技术和系统服务识别技术。端口扫描主要可分为全连接扫描、半连接扫描、秘密扫描、欺骗扫描等。

第三类技术主要有操作系统及服务检测技术。操作系统检测技术是利用好的网络扫描工具提供的响应列表，把收到的响应与列表中的响应进行对比，如果能与已知的某种操作系统响应匹配，就可以识别出目标主机所运行的操作系统的类型。这种技术主要有主动识别和被动识别技术。服务检测技术主要根据已扫描到的端口进行判定，或者利用 HTTP 响应分析、二进制信息探测等手段实现。

第四类技术主要有漏洞扫描技术。漏洞攻击是网络入侵的主要形式，攻击者的最终目的就是找到目标系统存在的薄弱环节，找到错误的配置或找出存在的危害性较大的系统漏洞。这些漏洞包括错误系统配置、弱口令、网络协议漏洞以及其他已知漏洞。漏洞扫描技术主要利用基于漏洞特征库匹配和插件技术实现目标系统漏洞检测。

## 5. 网络扫描算法

在实际扫描器编写过程中，除了有各种技术的选择，还需要选择合适的扫描算法。使用哪些扫描算法，也完全取决于扫描的目的，因为这些算法有些可以提高扫描效率，有些可以增加扫描准确度或扫描隐蔽性，有些甚至可能牺牲某些优点而获得所需要的特性。

### 1) 非顺序扫描

虽然通常使用增序扫描（即对所扫描的端口自小到大依次扫描），但是这一效果容易被对方发现。改变增序特征并不难，一般有以下几种非顺序扫描算法。

（1）逆序扫描算法。在扫描的时候，采用从大到小的逆序扫描方式。

（2）随机重排扫描算法。扫描端口的顺序可以用一个数组和随机数产生函数来实现。

（3）线程前加延时扫描算法。一个简单的算法就是在每一个线程中，扫描函数开始之前挂起一个随机的时间，这样会在不影响各线程创建时间的前提下，调整各线程中扫描的顺序。

### 2) 高速扫描

常见的高速扫描算法有多线程并行扫描技术、基于知识库技术、将扫描和判断分离的技术。多线程并行扫描技术是指对网上多组指令集、多条执行路径和多个执行单元同时进行扫描。基于知识库技术是指把扫描过的主机信息存储起来，当下次扫描的时候，首先以上次的扫描结果作为参考，对用户最关心的方面进行重新扫描，然后对其余部分进行扫描。将扫描和判断分离的技术是指将发送（扫描）和接收（判断）分开，发送只负责发送，接收操作统一进行，那么，由发出探测包到接收结果之间的等待时间成为并行，从而大大提高扫描速度。

### 3) 分布式扫描

高速扫描主要依靠多线程实现，而分布式扫描则主要使用多台主机同时对目标主机进行扫描，参与的主机可以事先约定后主动加入，也可以被入侵后植入扫描程序。在实施扫描的时候，由主控主机向各参与的主机发送要扫描的主机 IP 地址和端口范围，然后所有主机同时向被测主机进行扫描。

### 4) 服务扫描

端口扫描器只能扫描出端口的状态是否开放，而不会判断端口所对应的服务是否为该端口所具有的默认服务。服务扫描则是直接对服务进行扫描，并通过服务的存在与否，间接地判断端口是否处于“开”状态。同时，服务扫描本身也是一种需求。

### 5) 指纹识别算法

现在，操作系统种类繁多，版本更新的速度越来越快，想要了解某个远程主机的更多信息，可通过操作系统指纹识别算法判断对方所用的操作系统类型，甚至是版本号。所谓

指纹识别算法就是与目标主机建立连接，并发送某种请求，由于不同操作系统以及相同操作系统不同版本所返回的数据或格式不同，这样，根据返回的数据就可以判定目标主机的操作系统类型及版本。

#### 6) 漏洞扫描

漏洞扫描是指基于漏洞数据库，通过扫描等手段对指定的远程或本地计算机系统的安全脆弱性进行检测，发现可利用的漏洞的一种安全检测（渗透攻击）行为。主要有两大类：一是知识匹配法，二是模拟攻击法。模拟攻击法又有拒绝服务攻击、缓冲区溢出攻击、远程字典攻击等方式。

#### 7) 间接扫描

间接扫描的思想是利用第三方的 IP（欺骗主机）来隐藏真正扫描者的 IP。由于扫描主机会对欺骗主机发送回应信息，所以这种扫描的使用者必须具有监控欺骗主机的能力，以便获得原始扫描的结果。

#### 8) 秘密扫描

正常情况下的扫描有时会被对方的防火墙或 IDS 监测到，所以有些扫描器通常采用秘密扫描方式进行扫描。最典型的例子就是，扫描程序通过采用非正常和非常规的方式，试探协议中在网络较差情况下的容错技术，通过这些容错技术的不同反馈达到扫描的目的。这种方法由于没有完成正常的操作，所以对方不会认为是一种扫描或攻击，而只会认为是一次网络错误的发生，从而不会被记录下来，这相当于绕过了对方的安全机制，故名秘密扫描。

#### 9) 认证扫描

认证扫描则是利用认证协议的特性，通过判断获取到的监听端口的进程特征和行为，从而获得扫描端口的状态。认证扫描尝试与一个 TCP 端口建立连接，若连接成功，扫描器发送认证请求到目标主机的 TCP 端口，同时获取运行在某个端口上进程的用户名，以达到扫描的作用。

#### 10) 代理扫描

代理扫描需要在原有及所有算法的基础上再加上一个与代理服务器的通信，当前代理服务器的协议主要是 SOCKS5（它在使用 TCP/IP 协议通信的前端机器和服务器机器之间扮演一个中介角色，使得内部网中的前端机器变得能够访问互联网中的服务器，或使通信更加安全）。在代理扫描方式下，所有的扫描看上去像是对代理服务器扫描，因为所有数据都通过 SOCKS5 封装后发给了代理服务器，而代理服务器会将这些数据转发给被扫描的目标主机。这种扫描方式，在被扫主机看来，是由代理服务器本身在扫描自己，因而代理扫描难以反向跟踪。

### 11) 手工扫描

手工扫描是指在没有任何专用扫描器的前提下，只利用操作系统提供的命令或自带的程序文件进行扫描。当前主流操作系统都提供 ping、nbtstat、netstat、net 等命令，虽然这些命令都不具有扫描的特性，但通过这些命令却能或多或少地获得很多信息。

严格上说，手工扫描根本就不能算是一种扫描算法。因为这些程序本身算法各异，并且大部分命令只针对某一应用而做，很难显现“扫描”的特点。但考虑其在某种特殊场合下也许是唯一的选择，故也将其列为一种算法。

### 12) 被动扫描

以上几乎所有的扫描都属于主动探测模式，即发送刺探信息，然后根据对主机的反馈做出判断。被动扫描模式则不发送刺探消息，而只是监听。在这种模式下，扫描方从不或极少主动发送任何信息，而只是按协议被动地收集被扫描主机的敏感信息，最终达到扫描的目的。由于不主动发信息，所以对方无法反向监测，因此这是一种非常安全的方式。

## 5.3.2 网络侦听

网络侦听或称网络窃听，是指在网络接口处截获计算机之间通信的数据流，或指获取网络电缆上传输的所有网络报文的技术。网络侦听是常有的一种被动式网络进攻方法。当成功登录目标网络上的一台主机，并取得了这台主机的超级用户权限之后，往往要扩大战果，尝试夺取网络中其他主机的控制权，这时网络侦听就是一种最简单而且最有效的方法，它常常能轻易地获得用其他方法很难获得的信息，如用户口令、金融账号（信用卡号、账号、身份证号等）、敏感数据、低级协议信息（IP）地址、路由信息、TCP 套接字号等。

局域网是计算机网络的基本组成单元，广域网是由局域网通过广域信道连接形成的网络，广域网之间再互联就形成更大范围的网络，如互联网。局域网，如以太网、令牌网，都是广播型网络。也就是说一台主机发送信息时，网上任何一台机器都可以接收到这个信息。例如，以太网的介质访问控制（MAC，Media Access Control）协议采用 IEEE802.3 带冲突检测的载波多路监听（CSMA/CD，Carrier Sense Multiple Access with Collision Detection）协议，即在正常模式下，每台计算机的网络接口——以太网卡总是在监听网上发送的所有数据包，但仅当数据包的目的网卡（MAC）地址与自己的网卡地址相符时（表明数据包是发送给它的），才接收该数据包，并向上提交给本机协议栈进行处理；否则自动丢弃该数据包（表明数据包是发送给其他计算机的）。但是如果一台机器的以太网卡被设置成监听模式（或称混合模式、promiscuous），则以太网卡会接收监听到本网段上发送的每一个数据包，并向上提交给本机协议栈进行处理，而不管数据包是发送给谁的，这样

的一台计算机就成了网络窃听器（Sniffer）。以太网的窃听示意图如图 5-12 所示。

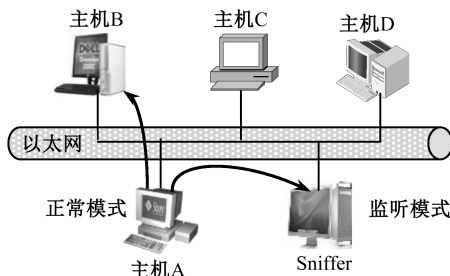


图 5-12 以太网的窃听示意图

网络侦听通常造成很大的安全危害，因为它们并不改变通信链路上的正常数据流，也不往链路上插入任何数据，所以很难被发现。

网络侦听可以在网上的任何一个位置实施，如局域网中的一台主机、路由器上或远程网的调制解调器之间等。但在网络上窃听效果最好的地方是在网络中某些具有战略意义的位置，如在网关、路由器、防火墙一类的设备或重要网段上。使用最方便的地方是在一个以太网中的一台上网的主机上，窃听用户的口令，这是大多数黑客的做法。

网络侦听常常要保存大量的信息，对收集的信息进行大量的整理工作。尽管网络窃听可截获和保存每一个数据包的所有信息，但这需要足够的存储介质。在一个网络流量很高的网络上，可能在很短的时间内，窃听器的输出文件会占满整个硬盘。因此，一个有效的方法是只截获和保存每一数据包的前 200~300 字节。一般认为，在数据包的头部会包括重要信息，如用户名和口令信息等，这是网络窃听真正想要得到的信息。

### 5.3.3 密码破译

密码破译是指利用计算机硬件和软件工具，从所截获的密文中推断出原来明文的一系列过程和行动的总称，又称为密码攻击或密码分析。密码破译可分为被动攻击和主动攻击两大类：仅对截获的密文进行分析而不对系统进行任何篡改称为被动攻击；密码破译后，如果采用删除、更改、增添、重放、伪造等方法向密文中加入假消息称为主动攻击。被动攻击的隐藏性更好，难以发现，但主动攻击的破坏性更大。

密码破译中有一个基本的假设称为 Kerckhoffs 假设，该假设假定密码破译者拥有所使用的算法的全部知识，密码系统的安全完全寓于密钥之中，也就是说，密码破译者除了不知道所使用的密钥之外，他了解整个密码系统。

根据进行密码破译的密码破译者所获得的信息类型，通常将密码破译分成以下四类：

(1) 唯密文破译。密码破译者拥有一个或更多的用同一密钥加密的密文，通过对这些

截获的密文进行分析得出明文或密钥。

(2) 已知明文破译。除待解的密文之外，密码破译者有一些明文和同一密钥加密这些明文所对应的密文，试图从中得出密钥。

(3) 选择明文破译。密码破译者可得到所需要的任何明文所对应密文，这些密文与待解的密文是用同一密钥加密得来的。

(4) 选择密文破译。密码破译者可得到所需要的任何密文所对应明文，解密这些密文所使用的密钥与解密待解的密文的密钥是一样的。

对密码破译者最为有利的条件就是选择明文破译。因此，好的密码算法必须能够经受得住选择明文破译。显而易见，这四种破译的强度是渐增的。

密码破译方法可分为穷搜索攻击、线性分析和差分分析等。密码史表明，密码破译者的成就似乎远比密码设计者的成就更令人赞叹。许多开始时被设计者吹嘘为“百年或千年难破”的密码，没过多久就被密码破译者巧妙地攻破了。在第二次世界大战中，美军破译了日本的“紫密”，使得日本在中途岛战役中失败。一些专家们估计，盟军在密码破译上的成功至少使第二次世界大战缩短了8年。

### 5.3.4 介质窃密

介质窃密主要包括电磁窃密和存储介质窃密。

#### 1. 电磁窃密

电磁窃密是利用各种电子侦察设备，对敌方计算机网络系统内各种电子设备所发射或辐射的电磁信号进行搜索、定位、检测、识别、记录和分析，获取对方计算机信息系统内的有关信息和情报。

在计算机网络中，计算机及其附属电子设备在工作时能把寄生电磁信号或谐波辐射出去，产生电磁辐射。这些电磁信号若被接收下来，经过提取处理，就可恢复出原信号。利用网络系统的任何一台电子设备工作时都会产生电磁辐射，计算机设备也不例外。计算机设备，包括主机、显示器、磁盘机、磁带机、终端机、打印机等所有设备所传递的数字脉冲信号都含有丰富的谐波，频谱可伸展到VHF和UHF范围，辐射能力很强，都会不同程度地产生电磁辐射，泄露信息。计算机信息电磁泄漏，主要有两种途径：一是被处理的信息会通过计算机内部产生的电磁波向空中发射，称为辐射发射；二是这种含有信息的电磁波也可以经电源线、信号线、地线等导体传送和辐射出去，称为传导发射。计算机电磁辐射尤其以带阴极射线管的视频显示器最为严重，屏幕上显示的信息，在很远的地方都可用高灵敏度电磁探测仪器，而不需要用复杂的分析技术就可以直接接收下来。1985年，荷兰电信总局的一名工程师在英国BBC电视台的配合下，进行了一次计算机终端信息辐射的窃听实验。窃收的目标是一条马路边楼内的一台正在工作的计算机终端，窃收装置放在路

边的一辆汽车里，窃收实验非常成功。在经过改装的电视机屏幕上，清晰地显示了楼内计算机终端工作的内容。这种侦察就已经不限于为网络进攻做准备，而是可直接从敌方计算机网络截获有关情报信息，所以也是一种被动网络进攻的方式。

## 2. 存储介质窃密

存储介质窃密是指通过有关网关手段获取对方用来存储信息的介质实体而得到有关的军事信息和情报。通常可以通过间谍、收买黑客、从第三者手中购买等手段。

计算机存储介质包括软磁盘、硬磁盘、磁带和光盘等，存储了大量的信息和各种秘密，已成为另一种“金库”和“机要室”。它的特点：一是信息储存量大、复制容易且不留痕迹。二是存储介质记录的信息，经过改写了的信息或抹除了的信息，经过特殊手段，都能复现出改写前的信息或抹除的信息。

## 5.4 网络空间作战态势感知模型

信息模型是网络空间作战态势感知系统各部分协同工作的公共数据基础，也是态势感知系统和其他相关作战系统进行数据交换的基础。为了确保作战态势信息在安全传感器、各级态势分析器之间准确地传递，并实现与预警和应急响应等系统之间的信息共享，必须建立公共的作战态势信息模型。即需要确定作战态势信息的组成要素和语义定义，要给出结构化的作战态势信息描述方法及规范，以此作为作战态势感知系统处理分析的数据基础，以及态势感知与应急响应等多个系统联动的公共数据基础。

### 5.4.1 网络空间态势感知的分析模型

从态势感知概念提出以来，研究者提出了各种各样的分析模型，其中影响最大，也最被普遍接受的是基于数据融合理念的模型。目前，大部分安全态势感知的模型都是基于美国的军事机构 JDL 给出的数据融合模型衍生出来的。图 5-13 展示了一个典型的网络空间态势感知模型。

在这个基于人机交互的模型中，态势感知的实现被分为了五个级别（阶段），首先是对 IT 资源进行要素信息采集，然后经过不同级别的处理及其不断反馈，最终通过态势可视化实现人机交互。五个处理级别分为是：

（1）数据预处理，可选的级别，对于部分不够规整的数据进行预处理，例如，用户分布式处理、杂质过滤等。

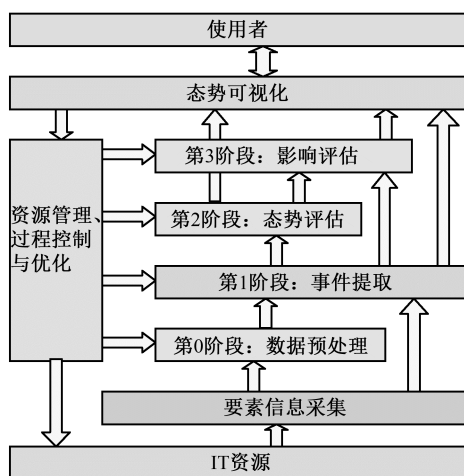


图 5-13 一个典型的网络空间态势感知模型

(2) 事件提取，是指要素信息采集后的事件标准化、修订，以及事件基本特征的扩展。

(3) 态势评估，包括关联分析和态势分析。态势评估的结果是形成态势分析报告和网络综合态势图，为网络管理员提供辅助决策信息。

(4) 影响评估，它将当前态势映射到未来，对未来战场或预测作战行为的影响进行评估。

(5) 资源管理、过程控制与优化，通过建立一定的优化指标，对整个融合过程进行实时监控与评价，实现相关资源的最优分配。

## 5.4.2 网络空间作战态势感知的功能模型

网络空间作战态势感知包括网络空间作战态势觉察、网络空间作战态势理解、网络空间作战态势投射三个层面。其中，态势觉察完成原始测量数据的融合与语义提取任务，以及活动辨识任务；态势理解完成这些辨识出的活动的意图理解任务；态势投射完成这些活动意图所产生的威胁判断任务。层与层之间存在依赖关系，即如果网络空间作战态势觉察和网络空间作战态势理解没有合理的结果，得到网络空间作战态势投射很可能也是不正确的或不完整的。但另一方面，每层的结果均可以独立呈现并直接使用，以满足不同的网络空间安全管理需要。这意味着网络空间作战态势感知的结果及其表达方式具有多样性，蕴含的语义粒度也可以随需求的视角而不同。但是无论如何，网络空间作战态势感知的结果应当是可响应的，否则缺乏实际意义。另外，网络空间作战态势感知是一个测量数据驱动的认知过程，测量数据的数量与质量影响感知的结果。

基于上述理解，网络空间作战态势感知一般功能模型可用图 5-14 来描述。该模型包



含网络空间作战态势觉察、网络空间作战态势理解、网络空间作战态势投射及可视化等模块，下面简要介绍各模块的功能。

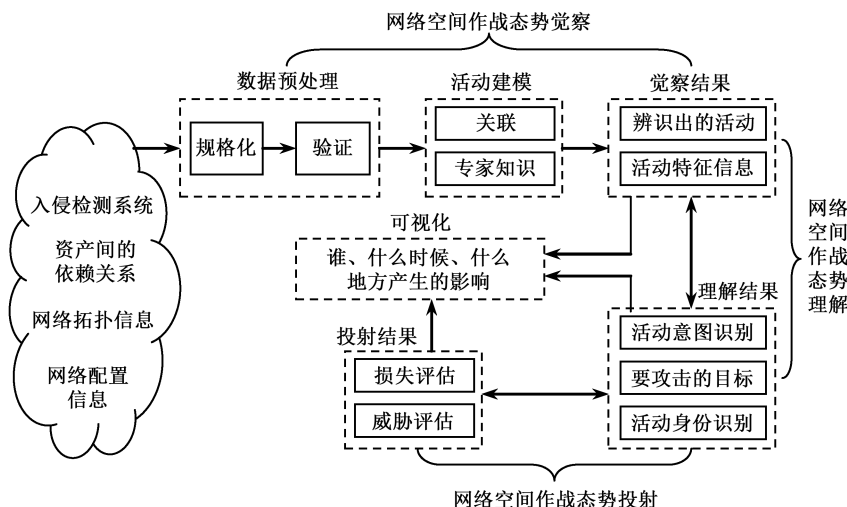


图 5-14 网络空间态势感知的一般功能模型

网络空间作战态势觉察主要目的是监视网络数据流，通过正常轮廓的学习，发现偏离正常轮廓的网络行为，辨识出系统中的活动，对网络中相关的检测设备与管理系统的原始数据进行降噪和规范化处理得到有效信息，然后对这些信息进行关联性分析，进而确定引起异常的入侵、入侵者身份、攻击的频度、攻击的威胁和进攻行为目的等。

网络空间作战态势理解的主要任务是在网络空间作战态势觉察的基础上，发现攻击活动的源头、类型，并判断攻击者的能力、机会和攻击成功的可能性等，理解并关联攻击活动的语义，然后在此基础上理解其意图。

网络空间安全态势投射的主要任务是在前两步的基础上，分析并评估攻击活动对当前系统中各个对象的威胁情况。这种投射包括发现这些攻击活动在对象上已经产生和可能产生（即预测）的效果。通过将态势感知的结果投射到确定的系统对象上，可以获得该对象在当前态势下的状态。尽管要感知的是系统中的活动，而感知的最终结果则应表达为这些活动对系统对象的影响，不能仅止于活动的识别，因为系统因之而产生的反应是施加于对象的，而不是直接施加于活动本身。这是一个再认识的过程，即融合从系统中观察到的各个对象的状态以构成态势，再看这个态势对系统各个对象的意义。

## 1. 网络空间作战态势觉察

网络空间作战态势觉察一般模型包含数据预处理、活动建模和网络空间作战态势觉察结果等三个功能，如图 5-15 所示。数据预处理完成测量数据的规范化和验证，有利于后续的融合处理。活动建模借助这些测量数据本身语义完成之间的关联性分析。觉察结果完成活动的辨识和特征提取。态势觉察是一个学习过程，因此活动建模和觉察结果之间存在反馈关系。

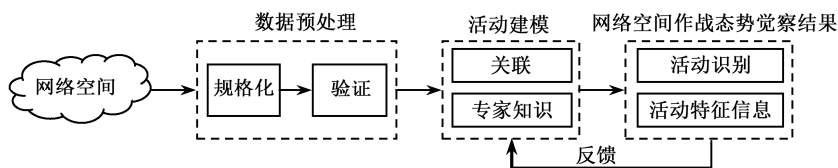


图 5-15 网络空间作战态势觉察一般模型

## 2. 网络空间作战态势理解

网络空间作战态势理解过程是建立在网络空间作战态势觉察，即网络空间作战事件检测基础之上的。根据识别出的攻击活动及其特征，通过进一步分析这些攻击活动的语义以及它们之间可能的关联关系来推断攻击者的意图。

作战态势的理解是融合、关联和归并作战事件信息，挖掘其蕴含的相互间逻辑关系，建立态势评价指标体系的过程。当前，在网络空间作战态势的理解过程中，使用了成熟的风险评估技术，利用风险评估理论对觉察到的安全事件进行风险量化分析，并利用基本元素的风险指标，建立定性或定量的评价指标体系，以此完成网络空间作战态势的理解过程，进而用定性或定量的结论完成对当前网络空间作战态势的解释。

## 3. 网络空间作战态势投射

网络空间作战态势投射一般模型由投射准备、风险评估技术和网络空间作战态势投射结果等三方面功能构成，如图 5-16 所示。投射准备将态势理解的结果映射到实际网络环境，确定被管对象面临的有效威胁。风险评估技术用来判断这些可能的威胁所产生的效果。态势投射结果综合判定系统中被保护对象面临的是什么样的实际威胁，以及威胁的程度与特点。

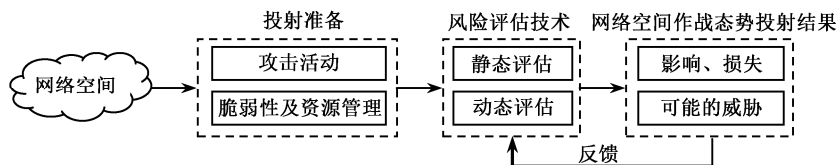


图 5-16 网络空间作战态势投射一般模型

静态评估是指在攻击发生之前，主动地分析和评估被管系统中存在的风险和隐患，支持全面预防性的安全响应决策。动态评估是指在攻击发生之时，基于当前的安全警报进行实时评估和预判型评估，以支持有针对性的动态安全响应决策。目前这方面的研究内容多集中在损失评估方面，即分析相关攻击活动对被管网络已经造成的危害。损失评估是指网络空间作战人员根据网络空间作战态势觉察识别出来的攻击活动和其他检测设备的报告内容，借助数学工具等模型，分析它对网络、系统资源等诸因素已经产生的影响。

### 5.4.3 网络空间层次化态势感知模型

与传统的态势感知不同,网络空间态势感知在范围、广度和深度上都极大地扩展了传统态势感知的范畴。首先,在感知范围上,网络空间的感知目标不仅包括物理实体空间,还包括虚拟社会空间,包括对人的心理、意识形态等要素的感知;在感知的广度上,网络空间态势感知涉及的目标对象更多,分布的区域更广,甚至涵盖全球范围;在感知的深度上,网络空间态势感知的认知对象不仅包括网络空间实体要素的外在状态、属性和动态等信息,还包括相关的环境要素、网络社会、行为特征等信息。具体地说,网络空间态势感知层次化模型如图 5-17 所示。

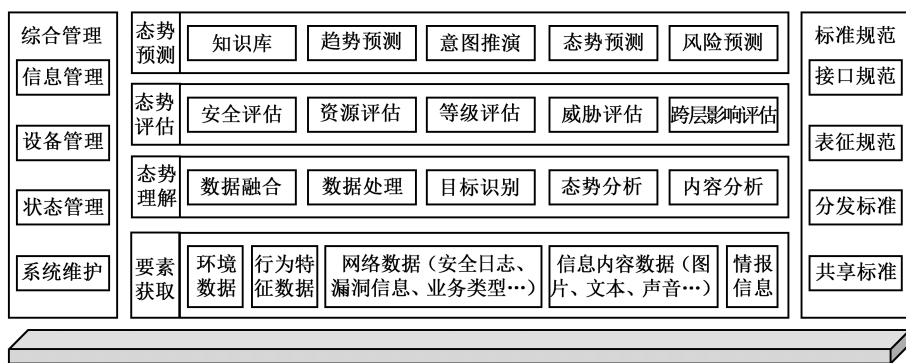


图 5-17 网络空间态势感知层次化模型

该层次化模型横向连通了网络空间态势感知的主要处理流程,由要素获取、态势理解、态势评估和态势预测四个阶段构成;纵向则贯穿了综合管理和标准规范两部分内容,为整个态势感知阶段的运行提供支撑保障。

态势要素获取是指综合采取网络侦察、情报、技侦等技术手段,通过主动与被动相结合的方式获取网络空间的网络数据、环境数据和行为特征数据等。针对网络空间监视区域广、覆盖面积宽等特点,态势要素获取需要考虑采用多传感器组合对监视区域空间分布式“采样”覆盖,时间上长时连续监视,关键技术包括传感器协同、传感器组网和动态交互等。

态势理解包括数据融合、数据处理、目标识别、态势分析和内容分析等。数据融合主要完成对多个信息源的数据进行自动监测、关联、相关、目标聚类处理,从而得到更为准确、全面的信息;数据处理主要是对来自传感器的数据进行初步处理,包括数据归并、数据格式转换和数据筛选;目标识别是在数据融合和处理的基础上,对目标进行初步分析;态势分析是将目标识别的结果归类为对手或我方,进行区别分析,进而综合形成当前安全态势;信息内容分析是通过对文本、图像和语音等信息内容进行关联分析,实现对意图、情报等的掌握。

态势评估是一个动态、智能的推理过程,通过分析网络中攻击事件之间的关联情况,

评估整个网络的当前安全态势，包括指标体系构建和态势评估。指标体系构建主要围绕网络指标体系、安全指标体系和网络进攻指标体系三个方面来进行；态势评估通过构建评估模型，定性定量分析当前网络空间的综合态势、安全状况和存在的薄弱环节，包括安全评估、资源评估、威胁评估等。此外，网络空间中由于目标复杂性，跨网络空间物理域、逻辑域和社会域各层之间的评估也是其中的关键环节。

态势预测包括知识库、趋势预测、风险预测和意图推演等。知识库涵盖网络进攻知识库、网络防御知识库，可为趋势和风险预测提供支撑；趋势预测从定性、时间序列和因果关系等角度出发，对网络空间态势的发展趋势进行预测和判断；风险预测是针对当前网络自身的漏洞和安全隐患，结合对手的态势发展，预测未来我方网络空间可能遭受的风险。

#### 5.4.4 可视化态势感知模型

态势感知为可视化的应用提供了理论框架，将可视化过程融入态势感知框架中，可形成相应的可视化态势感知模型，如图 5-18 所示。该模型包括五个阶段：态势感知（SA）需求分析、数据与知识提取、态势可视化与视图交互、态势感知、决策制定与执行。下面对每个阶段进行阐述。

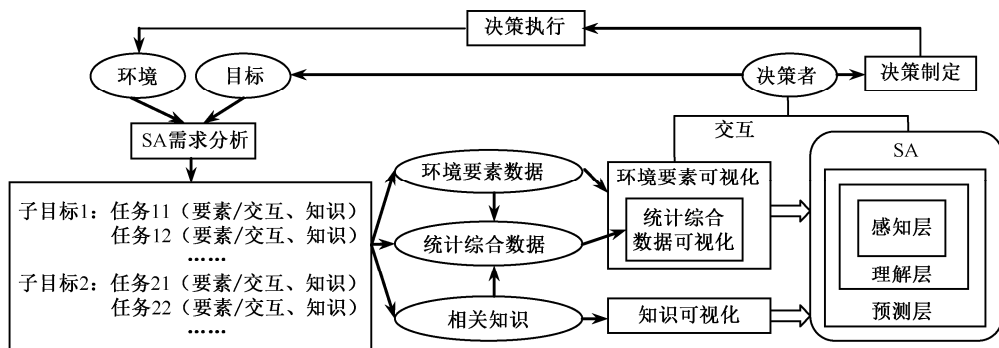


图 5-18 可视化态势感知模型

##### 1. 态势感知需求分析

要采用可视化技术支持态势感知，首先要进行态势感知需求分析，分析过程中要专注于环境本身和决策者的目标。态势感知的需求分析是一个逐步细化的过程，具体步骤如下：首先选取决策者，由其定义目标；对于较大的目标划分为具体的子目标；对每个子目标，为其划分任务（完成该目标要执行的任务）；定义每个任务所需感知的环境要素、要执行的交互行为和应具备的知识。态势感知需求分析是进行态势感知可视化的基础，它界定了可视化的数据源、可视化视图和视图交互的范围与内容。

## 2. 数据与知识提取

这一阶段要采用各种方法和技术提取：环境要素数据，环境要素的各类统计和综合数据，决策活动中积累下来的、态势感知过程中所需的相关知识。这些数据与知识在提取完成后以标准数据表的形式存储。

## 3. 态势可视化与视图交互

在第二阶段形成的标准数据表的基础上，采用各种可视化技术对环境要素、统计综合数据和相关知识进行可视化。可视化的流程符合通用信息可视化流程，但在可视化数据的类型、可视化视图的多视图特征、可视化视图的交互上要符合决策者态势感知的需要。可视化功能的实现应以任务为中心，为同类任务设计可视化视图，采用多视图策略，将完成该任务所需的环境信息、要素信息、统计综合数据和知识按照视图间的关联性、解释性、逻辑性和过程性进行组织，并提供视图交互功能。

## 4. 态势感知

决策者根据决策目标和任务与可视化视图交互，进行态势感知。环境要素可视化是三级态势感知基础；统计综合数据可视化则为理解层的基础；知识可视化作为解释性、支撑性的功能，是对决策者知识的外化，需要支持全部三层态势感知，尤其对理解层和预测层的支持，因为这两层需要充分利用决策者的相关知识。

## 5. 决策制定与执行

通过与可视化视图的交互，决策者进行了充分的态势感知后，开始进入决策制定与执行阶段，执行过程会改变决策者所处的环境，而目标也会因为决策执行的完毕发生新的变化。环境和目标的变化，要求重新进行态势感知需求分析，对目标、任务、交互操作进行新的分解，回到第一阶段，开始新的可视化感知流程。

# 5.5 网络空间作战态势感知的体系结构及其组成

网络空间作战态势感知的体系结构是指网络态势感知的各组成部分及其本身所必须实现的功能的精确定义，是网络态势感知中的层次、各层的协议以及层间的接口的集合。它为系统的整体设计，网络硬件、软件、协议、存取控制和拓扑的应用提供参考依据。

## 5.5.1 体系结构

网络空间作战态势感知体系结构由主动探测与被动监测相结合的数据采集、面向网络

攻防博弈的安全态势评估、基于网络威胁的安全态势预测三部分构成，如图 5-19 所示。

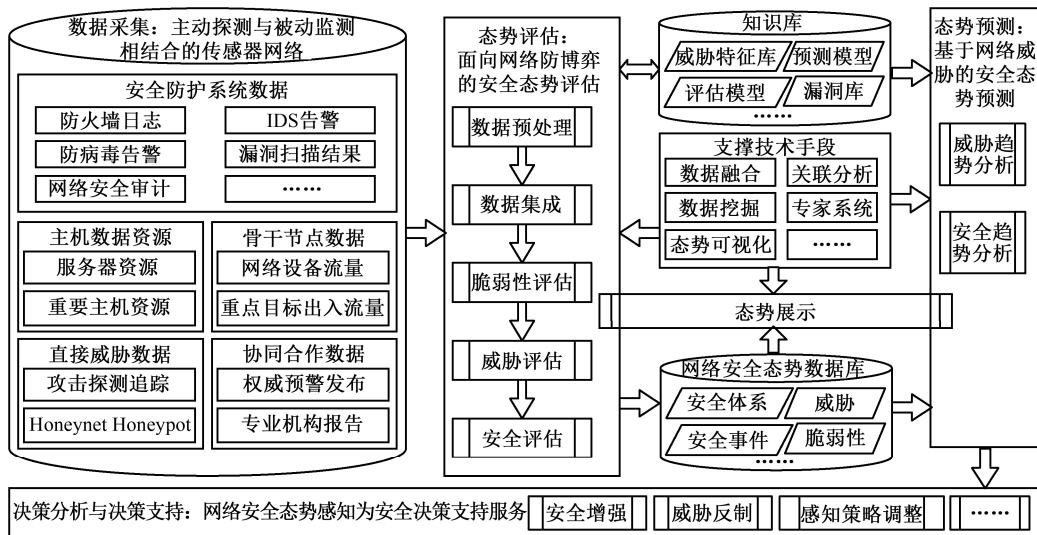


图 5-19 网络空间作战态势感知体系结构

## 1. 数据采集

传感器网络通过主动探测与被动监测相结合的态势要素采集数据，针对以下五种类型的数据：一是来自网络空间安全防护系统的数据，如防火墙、IDS、漏洞扫描与流量审计等设备的日志或告警数据；二是来自重要服务器与主机的数据，如服务器安全日志、进程调用和文件访问等信息，基于网络与基于主机的协同能够大大提升网络威胁感知能力；三是网络骨干节点的数据，如电信运营商管理的骨干路由器的原始网络数据，网络节点数据采集的越多，追踪、确认网络进攻路径的可能性就越大；四是直接的威胁感知数据，如 Honeynet 诱捕的网络进攻数据，对网络进攻源及攻击路径的追踪探测数据；五是协同合作数据，包括权威部门发布的病毒蠕虫爆发的预警数据，网络空间安全公司或研究机构提供的进攻行为分析报告等。

除了第一、第二种类型数据的采集，后面三种类型的数据采集都体现了积极主动的安全态势感知。如果通过某种方式拥有骨干网络设备的控制权，借助设备的镜像等功能，就能够获取流经网络设备的特定数据。曾经斯诺登披露的美国国家安全局“棱镜”计划中就有利用思科路由器的“后门”，获取境外骨干网络节点数据的内容；而且，该计划要求一些公司提供有关数据，来完善其监控信息。

## 2. 安全态势评估

评估分为数据预处理、数据集成、脆弱性评估、威胁评估和安全评估五个步骤。对异构的传感器数据，需在数据分类的基础上进行格式归一化处理，然后在相关知识库与技术手段的支撑下，根据对威胁、脆弱性或安全事件等的标志，进行数据去重、集成和关联，再依次进行面向脆弱性、威胁和安全性的专项评估。由于当前数据集成与融合的相关

技术尚不完善,这里侧重于以威胁识别为牵引,来评估因为威胁变化而引发的安全状态变化,即面向网络攻防对抗的作战态势评估。为此,需解决三个基础问题:

(1) 对网络威胁主动探测数据的利用。这些数据虽然可能不完整、不系统,但指向性很强,能够明确作为威胁存在的证据,可用于确认安全事件、新威胁发现和攻击路径还原。

(2) 将宏观的骨干网络节点数据与具体的涉及某个信息系统的数据进行关联。从具体的数据中提取关键字段,比如 IP 地址或攻击特征,然后基于这些字段在宏观网络数据中找出相关的数据,解决宏观与微观数据的关联问题。

(3) 从海量网络数据中提取可疑的网络进攻行为数据。以特征匹配技术为支撑,深化攻击模式与数据流特征提取,提升对新威胁的监测能力。

### 3. 安全态势预测

相对于脆弱性的出现与安全策略的调整,网络威胁的变化频率要高很多。因此,在全面获取网络威胁相关状态数据的情况下,想定不同的场景和条件,根据网络空间安全的历史和当前状态信息,基于网络威胁来进行态势预测,就能够较好地反映网络空间安全在未来一段时间内的发展趋势。态势预测的目标不是产生准确的预警信息,而是要将预测结果用于决策分析与支持,特别要上升到支持网络攻防对抗的层次上。

## 5.5.2 态势感知系统分析架构

网络空间态势感知系统包含事件采集、事件预处理、事件关联分析、指标体系提取、态势评估等,具体的系统分析架构如图 5-20 所示。

### 1. 事件采集

网络空间作战态势感知系统中部署的每一种安全设备都有相匹配的代理程序 Agent,该代理程序实时监听安全设备数据,一旦安全设备有新数据生成,Agent 负责将安全事件提交至服务器端,没有新数据生成代理设备 Agent 休眠一定时间,接着监听安全设备有无新的数据生成,重复前面的流程。该事件采集过程如图 5-21 所示。

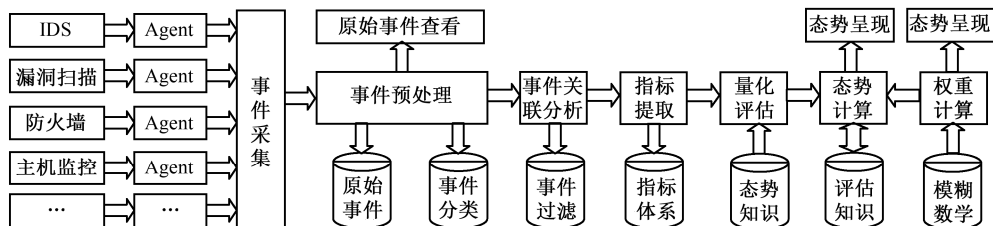


图 5-20 网络空间作战态势感知系统分析框架

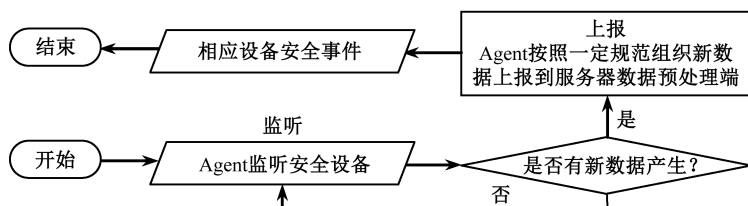


图 5-21 事件采集过程

## 2. 事件预处理

服务器端事件预处理模块负责接受代理端上报的安全事件，然后对不同安全设备代理上报的安全事件进行预处理，将安全事件格式统一，作为构建指标体系和态势评估的数据源。事件预处理过程如图 5-22 所示。

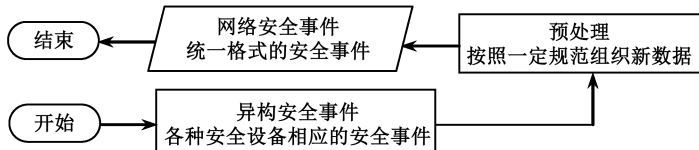


图 5-22 事件预处理过程

## 3. 事件关联分析

对不同安全设备上上报的经过预处理的安全事件进行关联分析，包括两部分：事件交叉关联和事件动态关联。经过事件关联分析实现对重报、误报安全事件的过滤，减轻后面指标提取及量化评估的工作量。事件关联分析过程如图 5-23 所示。

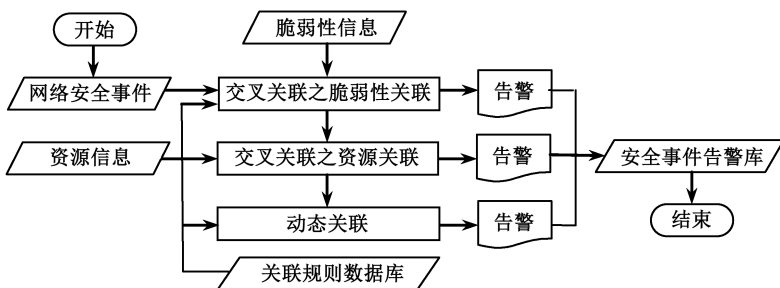


图 5-23 事件关联分析过程

## 4. 权重计算

权重计算主要功能是计算下层所有评估因素相对于上层评估对象的重要性程度，按照模糊层次分析法建立子层相对父层的模糊互补矩阵，根据模糊互补矩阵性质调整模糊互补矩阵使其具备一致性。权重计算数据流程图如图 5-24 所示。



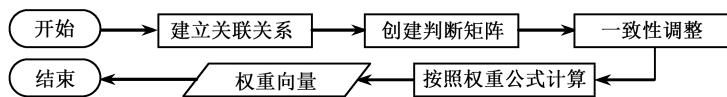


图 5-24 权重计算数据流程图

## 5. 态势计算

态势计算是指根据之前建立评估模型,对当下一定时间窗口内经过处理的安全事件信息和相应的权值信息,展开计算得到当下系统及各维态势指数。态势计算过程如图 5-25 所示。

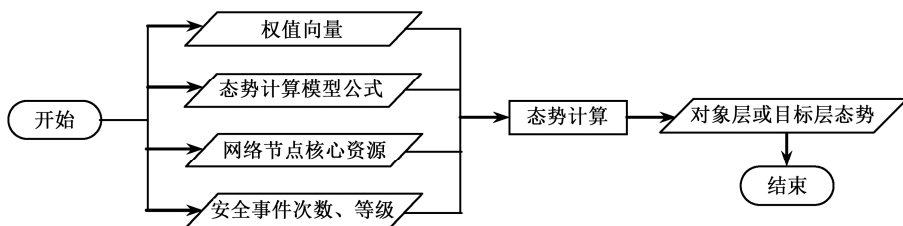


图 5-25 态势计算过程

## 6. 态势呈现

态势呈现是将前一个态势计算模块计算的结果以报表、折线等多种形式呈现给用户,方便用户清楚地获知当下网络的各维态势及系统的综合态势信息。

### 5.5.3 态势感知支撑平台的组成

在网络空间作战态势感知体系框架的基础上,以测试评估流程为主线,以管理控制为中心,以测试评估数据为基础,构建态势感知支撑平台。支撑平台由三个分系统和一个数据中心组成,分系统包括管理控制分系统、安全测试分系统和态势感知分系统。其中,管理控制分系统包含用户管理界面、安全管理、任务管理、数据管理和工具管理等管理控制子系统;安全测试分系统由资源识别、脆弱性检测、恶意代码检测、渗透测试、安全设备在线测试和安全事件验证六个子系统组成;态势感知分系统包含安全态势评估和预测子系统。各分系统和数据中心通过统一的任务分发接口、数据收集接口和数据访问接口进行交互。态势感知支撑平台的组成及其相互关系如图 5-26 所示。

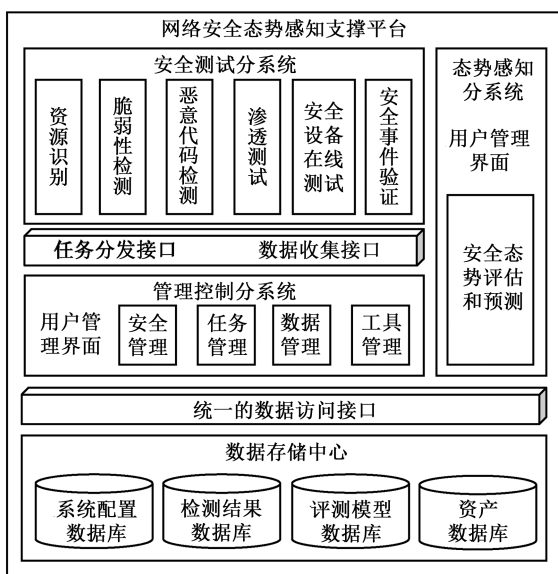


图 5-26 态势感知支撑平台的组成及相互关系

下面对支撑平台核心的三个分系统进行介绍。

## 1. 管理控制分系统

该系统以管理控制子系统的形式存在，是支撑平台的管理控制中枢，负责测试评估项目和数据的管理，以项目、任务、子任务的层次结构来对测试评估项目和数据进行统一的管理，并建立中心数据库对测试评估数据进行归档和存储。

## 2. 安全测试分系统

该系统采用多种检测技术和手段，采集网络空间作战相关元素，其六个子系统的功能如下：

(1) 资源识别子系统，负责对网络信息系统中的有形或无形资源进行识别，对资源的保密性、完整性和可用性进行赋值，以调查问卷、实地查看等方式记录资源。

(2) 安全设备在线测试子系统，负责识别网络信息系统中安全设备的运行管理脆弱性，对防火墙、安全网关、统一威胁管理设备、IDS 等安全设备进行实时在线或离线的安全检测，以定制有状态的网络会话和网络进攻会话穿越受检设备的方式，来测试安全设备是否存在策略配置、抗进攻渗透和升级更新等方面的脆弱性。

(3) 脆弱性检测子系统，负责识别网络信息系统中软硬件固有的安全漏洞，通过网络扫描的方式，对存在 IP 地址的物理实体检测操作系统、通信协议、应用软件、数据库等是否存在已知的安全漏洞。

(4) 渗透测试子系统，负责验证已存在的脆弱性和软硬件固有安全漏洞对网络信息系统的危害程度，根据在线测试、脆弱性检测和恶意代码检测获得的结果，通过漏洞利用等

进攻手段验证安全漏洞及恶意代码的危害程度。

(5) 安全事件验证子系统, 负责验证网络系统中已发生的安全事件, 利用脆弱性检测、在线测试、恶意代码检测等子系统的检测数据, 以及 IDS 和防病毒系统的告警数据, 通过采集网络数据和主机数据的方式, 进行数据层面的协同融合, 来确定安全事件的存在及其影响。

(6) 恶意代码检测子系统, 负责检测网络中的主机是否存在木马、蠕虫、间谍软件、僵尸网络代理程序等恶意代码, 通过特征匹配和行为异常法, 利用主机资源信息进行检测。

### 3. 态势感知分系统

该系统以态势评估和预测子系统的形式存在, 根据测试数据对网络进行定性和定量的安全评估和安全趋势预测, 依据国家相关标准和规范, 利用测试数据和相关评估模型, 对网络进行安全评估, 通过报表方式, 对测试评估结果进行表示。

各子系统采用松耦合结构, 以数据交互为联系方式, 能够独立进行测试或评估。这里使用控制、数据、协同三种类型的接口来支持各子系统之间的交互, 把控制、数据和协同设计为通用的控制接口。数据接口用于管理控制子系统与其他子系统的交互, 负责测评任务分发提交和测试评估数据传输; 协同接口用于除管理控制和安全态势评估与预测两个子系统之外的其他子系统间的交互, 负责测试任务的协作, 各个检测子系统相互独立进行工作, 只通过协同接口互相联系, 以获取自己测试所需要的信息。支撑平台子系统之间的交互接口如图 5-27 所示。

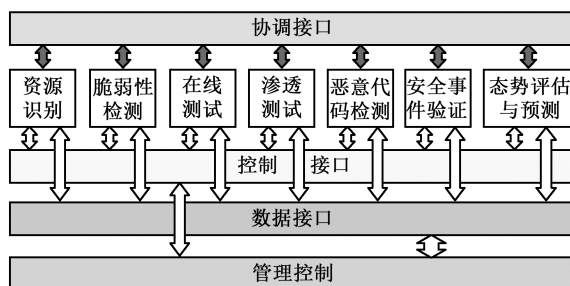


图 5-27 支撑平台子系统之间的交互接口

资源识别、在线测试、恶意代码检测和脆弱性检测四个子系统属于基础检测子系统, 不需要从其他子系统获取信息, 但要给其他子系统提供测试数据。渗透测试、安全事件验证两个子系统在开始工作之前, 应从其他测试子系统获得必要的信息。渗透测试子系统不但需要在线测试子系统提供有关防火墙、IDS 等设备的脆弱性数据, 同时需要恶意代码检测子系统提供木马、间谍软件等威胁数据, 还需要脆弱性检测子系统提供安全漏洞等脆弱性数据; 而安全事件验证子系统不但需要恶意代码检测子系统提供木马、间谍软件等威胁数据, 同时需要脆弱性检测子系统提供安全漏洞等脆弱性数据, 还需要验证 IDS、防病毒系统的告警数据。态势评估与预测子系统利用六个检测子系统得到的检测数据进行网络空间作战态势的分析。

通过这些接口，相互独立的子系统能够集成为一个综合的支撑平台，第三方成熟的测试评估手段也能够融入支撑平台中来。控制、协同两个接口采用基于移动存储介质的文件传输方式，通过 XML 文件进行子系统间的交互，数据接口基于 TCP/IP 协议进行测试评估数据传输。

由于测试评估技术的不断发展，导致难以研制完整的支撑平台，因此在支撑平台建设时，应遵循大框架、小平台的原则，子系统之间具有清晰明确的接口，使检测方法、工具和评估模型具有良好的可扩展性，便于升级和维护。最终建成的支撑平台是个分布式的安全测试评估系统，具有开放的体系结构，通过自定义的互操作接口，给新的安全测试评估手段集成提供高效统一的方案，从而有效提高网络空间作战态势感知水平。

## 5.6 网络空间作战态势感知系统的设计

### 5.6.1 设计原则和目标

#### 1. 设计原则

在软件设计过程中，需求分析和系统设计是生命周期内的两个关键过程，怎么把需求转化为系统设计，影响着软件的质量。因此在设计网络空间作战态势感知系统框架结构时，需要遵循以下原则：

(1) 安全性。系统运行在网络中，必须确保所传送的数据不被窥视和篡改，并且要防止非法用户对网络资源或私有信息的访问。

(2) 高效性。由于网络结构的复杂性和带宽本身非常有限，流量高峰时期常常出现阻塞，在网络数据采集的过程中，需要保持较高的数据采集效率，确保系统的安全运行，以保证能较快地发现网络范围内的安全威胁并做出处理，防止网络系统受到进一步破坏。

(3) 实时性。网络空间安全管理的一个重要方面就是在动态环境下及时发现系统遭受到的威胁，采取相应的措施或策略来确保系统安全，在感知过程中的各个处理过程都要具有实时性，准确反映网络系统运行状况。

(4) 开放性。由于网络环境中包含网络设备、安全设备、存储设备、主机和终端设备等，系统应能够集成各种异构信息。

(5) 可扩展性。网络空间作战态势感知系统是一个管理支撑平台，系统必须有较好的可扩展性，这就需要设计灵活的接口形式及可拓展的网络空间安全集成平台。采用组件化设计思想，用户可以选择和配置所需的组件，实现新功能的动态增加。

(6) 跨平台性。系统需要适应多种操作系统。

(7) 健壮性。系统有多个功能模块共同完成网络空间作战态势的感知过程, 应该降低一个模块对其他模块的依赖性, 同时采取响应的备份措施, 确保系统的健壮性。

(8) 易操作性。安全管理人员只需根据具体网络环境进行简单的配置就能达到监控整个网络空间作战态势的目的。

## 2. 设计目标

网络空间作战态势感知系统的设计目标可简要地描述为:

(1) 能实时监控和采集网络、服务、系统软件以及应用的安全状态数据, 及时发现网络进攻行为或其他作战异常, 支持大规模网络的作战态势感知。

(2) 能融合、关联来自多种作战事件源的海量数据, 通过综合分析判断网络进攻和其他事件的类型, 确定进攻行为的性质和可能造成的影响, 及时有效反馈作战态势数据信息, 预测网络的未来发展趋势, 并及时报警和预警。

(3) 能集中监控系统的作战态势, 融合生成全局作战态势, 提供多角度多尺度的作战态势表示, 实现统一态势图的集成。

(4) 能提供准确的网络空间作战事件基础数据库。

(5) 完成对网络中设备信息的配置并对网络设备进行信息获取。

(6) 采用 B/S 架构为网络管理人员提供可视化的管理界面, 系统管理员可以通过 Web 页面进行远程控制, 提高管理效率。

(7) 支持网页浏览器 (IE, Internet Explorer)、搜狗、360 等主流浏览器。

(8) 实现对网络空间作战态势数据及设备数据的客观和逼真展示。

(9) 系统管理员根据系统的事实状况开启定时计划功能, 同时进行服务控制, 有效减少系统占用资源。

(10) 形成操作日志, 方便管理员进行管理。

(11) 实现网络空间作战态势告警信息的显示。

### 5.6.2 系统功能需求分析

网络空间作战态势感知是实现安全要素的获取、理解、显示, 以及对未来安全发展趋势的预测和评估。安全要素包括数据和环境两部分。数据主要包括两方面的信息数据: 一是由入侵检测系统、安全审计系统、漏洞扫描系统、防火墙等安全防护系统和设备产生的信息数据; 二是由终端、服务器、交换机、路由器等网络设备因安全事件而产生的信息数据。环境则包括了由设备所构成的软硬件环境以及由用户操作形成的用户行为环境。依据上述所给出的概念、设计原则和目标, 网络空间作战态势感知系统应该具有的基本功能包括网络集中监控、文件集中管理、设备的有效管理、数据处理、分域分析、决策分析、设备自动发现。

## 1. 网络集中监控

一个网络环境中包括网络设备、安全设备、存储设备、主机、终端设备和各类应用，并且各个设备和应用都有独立的管理工具，操作不方便，信息无法共享。在这种情况下，首先要解决网络空间安全管理中的透明性问题，全面获取网络空间安全实时状态信息，实现对各种设备的安全日志统一监控；其次是解决网络空间安全管理中的可管理性问题，安全人员能在统一平台界面上监视整个网络中各个域内的安全状况，克服管理中分散、非实时问题。

## 2. 文件集中管理

各设备的配置文件集中管理，安全策略的统一分发、修正和更新，配置文件的统一在离线管理、定期采集与审核，对各个设备的属性和策略进行集中的存储、查询。由于目前普遍使用的 IDS、Firewall 和病毒检测系统（VDS，Virus Detection System）等往往各自为政，通常需要同时运行多个控制端，这造成了管理和监控的不便，采用集中管理可以提高维护管理水平和效率。

## 3. 设备的有效管理

建设网络态势感知的最根本目标就是最大限度保证设备资源的运行安全和使用安全。这里的设备包括所有的安全防护设备和网络设备，对设备的管理主要包括以下三个方面。

（1）设备登记管理。资源的“入库”是系统能够正常开展工作的第一步。通过手工录入、系统扫描或外部导入等方式，可把新的资源信息登记到网络空间态势感知系统中。必要时可对已入库的资源进行信息修改、删除等操作，实时反映系统里资源的在册状态。

（2）设备拓扑管理。以图形化形式展示资源的连接状态。可以创建、修改、删除拓扑图，设置图形上的设备和真实设备之间的映射关系，以反映单个设备、区域范围内的设备、全部范围内的设备等不同范围设备之间的连接关系。

（3）设备归类管理。以分组的形式将所有设备划分为功能相对一致的设备群，以实施对设备群的可用性监控，包括服务状态监控、主机监控、故障监控等。

## 4. 数据处理

作战数据处理主要包括四部分内容：数据采集、数据转换、数据聚合和数据关联。

（1）数据采集的主要功能是设置和配置数据检测器和采集器，实时检测网络空间态势感知各设备的报警信息和日志信息，采集被检测数据。

（2）数据转换的主要功能是将有效的采集信息数据转换成统一的报警数据标准格式，并存储于数据库里。

（3）数据聚合的主要功能是对报警信息进行分类，并对同一类的原始报警信息进行聚合，形成超报警信息。

（4）数据关联的主要功能是确定同一进攻行为发生的先后次序（步骤），并对相关报

警信息进行关联，形成完整进攻过程。

### 5. 分域分析

分域分析完成各个域内的安全要素提取功能，包括局部分分析和全局分析两部分。局部分分析对象是域内各个传感器所提供的安全数据，而全局分析对象覆盖了各个域内的安全数据，通过聚类 and 融合方法提取相应的安全态势要素，并在一定程度上精简数据和识别进攻，为上层决策分析提供数据支持。

### 6. 决策分析

决策分析是对局部和全局分析结果进行综合理解的过程，包括当前网络空间作战态势评估和未来安全态势预测两部分功能。通过决策分析使得安全管理人员更加便捷地掌握整个网络的安全状况，为制定全局策略提供必要的依据。

### 7. 设备自动发现

自动设备发现功能主要完成网络中设备的探测和更新任务，一旦网络拓扑发生变化，系统便能够自动发现设备的调整并给出基本的探测信息。由于大部分网络的拓扑都是变化的，如果不支持设备的自动发现，就需要人工方式解决，给管理员造成较大的工作压力，使其无法掌握网络的实际拓扑，这样不便于排错和发现安全故障。为此可以采用自动搜寻拓扑的机制，如通过更改工具库，来随时识别新添加的设备。

## 5.6.3 网络空间作战态势感知系统总体架构的设计

在明确系统功能需求的基础上，参照设计原则要求，设计出如图 5-28 所示的网络空间作战态势感知系统总体架构。该结构是一个分布式开放结构，采用的主要思想是“分布式获取，分域式处理”，可分为信息获取层、要素提取层和态势决策层三个层次。信息获取层通过部署所设计的日志类传感器、简单网络管理协议（SNMP）传感器、NetFlow 传感器和服务传感器，获取网络环境中主机、交换设备、安全设备等各种异构信息。要素提取层针对所获取的各种异构信息，采用聚合和融合方法对其进行必要的的数据精简和安全事件提取。态势决策层采用层次评估思想和非线性时间序列预测方法分别完成多源信息的综合理解和动态预测，为上层用户提供直观的安全态势视图。信息获取层、要素提取层和态势决策层的实现都需要与相应的数据库进行交互。数据库包含有事件库、关键资源库、网络信息库、知识库等，这些数据库的形成需要专家、安全管理人员及网络扫描器等进行辅助。在后续几节中将详细地给出各层的模块设计。

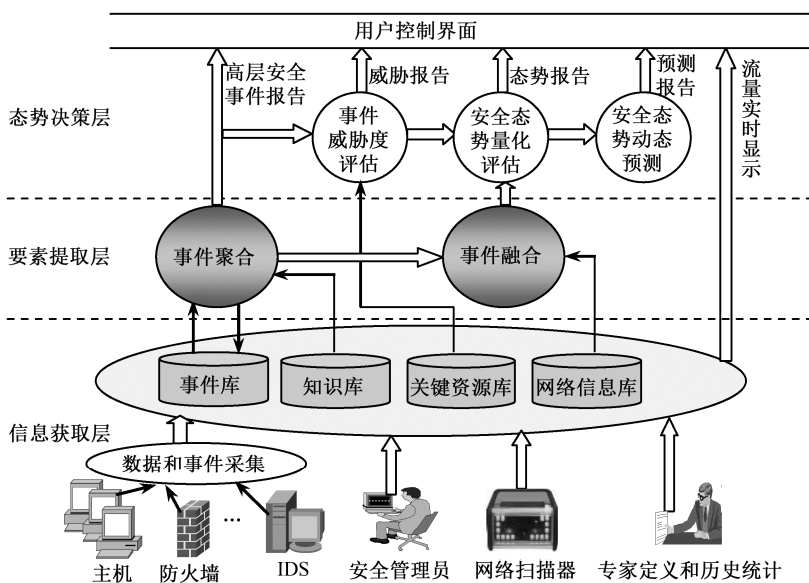


图 5-28 网络空间作战态势感知系统总体架构

#### 5.6.4 信息获取层的设计

信息获取层位于系统框架结构底部，其主要职能是获取当前网络状况及预测未来趋势所需的态势信息，在系统中发挥着基础性支撑作用。信息获取层可进一步细分为三个子层，分别是设备层、传感器层和信息集成层。信息获取层结构如图 5-29 所示。信息获取层的结构采用了分层设计，通过封装各子层的实现细节，分层可保证各子层的相对独立性和透明性，减少各子层的耦合性；与此同时，各层之间通过自底向上的数据流和自顶向下的命令流有机融合为一个整体。

设备层是原始数据的来源，设备层设备的选取取决于数据源的选取以及系统目标网络的设备安装和部署情况。传感器层由多种类型的传感器组成，各传感器之间存在一定的数据互补性，比如基于 NetFlow 的传感器在判断端口异常时需要知道端口被哪个程序使用，而 NetFlow 传感器无法获取这样的数据，日志传感器却较容易获得。针对这一需求，各传感器间预留交互接口，使得传感器间能够共享必要的信息，有助于提高传感器获取信息的全面性和准确性。此外，为了获得更好的可扩展性，传感器层应采用统一的接口规范，满足该接口规范的传感器都可以加入传感器层中。信息集成层具有集成和初步融合来自各传感器的初步信息、安全事件的功能。另外，由于上层应用需要针对特定安全事件查询判定该安全事件的相关数据，因此信息获取层还需要提供一个面向上层应用的查询响应接口，通过该接口接收和解析上层应用的查询命令，并从安全事件库或传感器初步信息库及原始数据库中查询数据并返回。为了使得信息获取层对上层应用透明，只在信息集成器提供面向上层应用的查询响应接口。



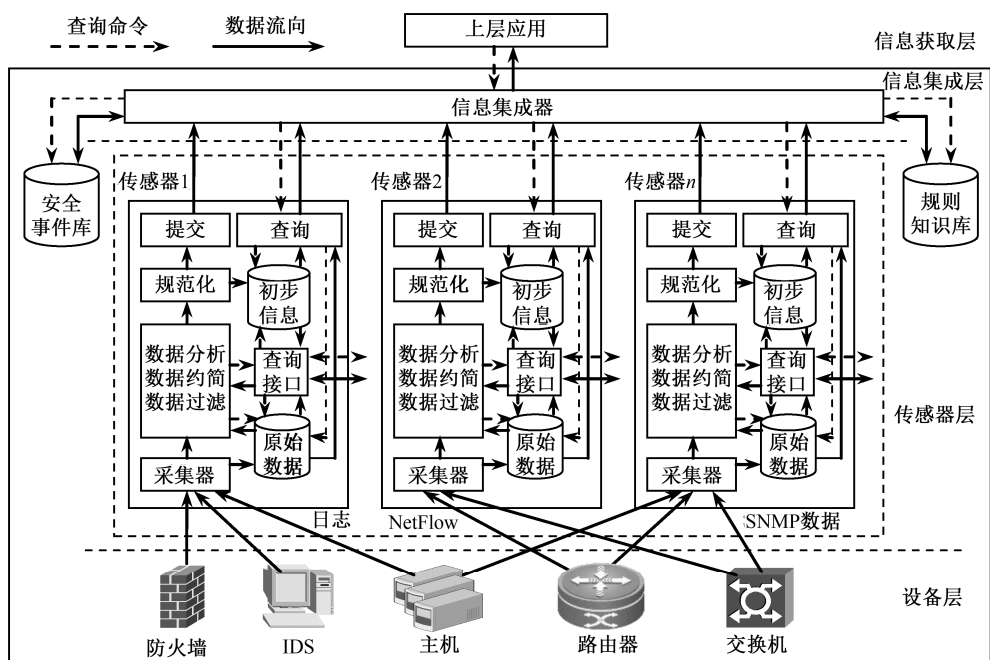


图 5-29 信息获取层结构

### 5.6.5 要素提取层的设计

要素提取层对信息获取层得到的各种异构信息，采用聚合和融合方法进行数据精简和安全事件提取。图 5-30 给出了大规模分布式网络空间安全要素提取结构图，主要分为局部分分析和全局分析两大部分。局部分分析是在各安全域传感器所获取的信息基础上，首先对其执行 XML 格式化，再采用基于相异度计算方法对其进行局部聚类分析，并对聚类后的结果采用基于指数加权的 DS (Dempster/Shافر) 证据理论进行融合关联，最终提交到全局分析模块，采用相同的聚合和融合方法完成全局聚合和融合，经过局部分分析和全局分析后便完成了对安全要素的提取。

#### 1. 多源异构安全信息聚合

要素提取层首先对多源异构安全信息执行聚合操作，聚合的流程如图 5-31 所示。安全信息读取模块从数据库中读取已格式化的安全信息，输入到相异度计算模块，依据每条标准化安全信息的特征属性分别与分类模板中结果进行比较，并将结果输入到聚合判决模块中，判断满足闭值条件的安全信息划分为同一类别。支持数据库主要有 4 个，分别是标准化安全信息库、分类模板库、权值库、域值库。分类模板库主要用于指导属性相异度计算和聚合判决，并接收聚合判决更新结果；权值库依赖于专家经验，一般采用模糊综合评判方法及时更新；域值库依据历史统计数据给出不同字段对域值的要求。

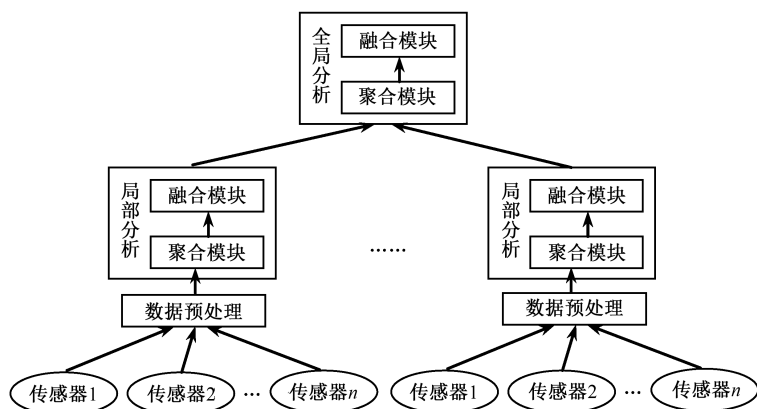


图 5-30 网络空间安全要素提取结构图

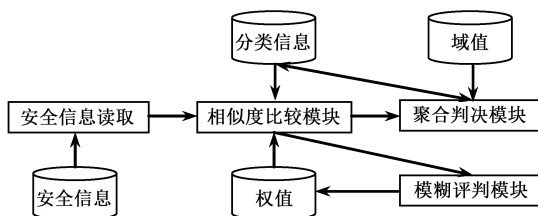


图 5-31 多源异构安全信息聚合流程

其中所考虑的特征属性主要有源目的 IP、源目的端口、检测时间、进攻类别等，分别计算其相异度，最终计算出综合相异程度。

## 2. 多源异构安全信息融合

对安全信息执行聚合之后，采用基于指数加权 DS 证据理论对聚合结果进行融合分析，旨在进一步精简安全信息数量和识别进攻行为。多源异构安全信息融合流程如图 5-32 所示。从分类信息库中获取安全事件信息，并依据不同传感器的检测率配置信度；传感器权重分配模块依据进攻情况，获取各个传感器的权值；DS 推理模块

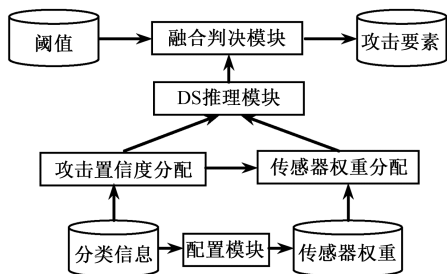


图 5-32 多源异构安全信息融合流程

根据不同传感器具有的不同重要性，综合理解进攻行为发生的概率，给出推理结果并提交至上层的融合判决模块，判决模块依据阈值要求得出相应的结果，存入数据库中，即完成安全要素提取。整个过程主要涉及 4 个数据库，分别是安全事件分类信息库、传感器权重库、判决阈值库和安全要素库。安全管理人员可以依据对当前和历史安全事件信息的统计和分析，并结合不同安全域的重要性，动态更新配置传感器权重库。

### 5.6.6 态势决策层的设计

态势决策层主要由事件威胁度评估模块、安全态势量化评估模块和安全态势动态预测模块构成。

#### 1. 事件威胁度评估模块

事件威胁度评估模块是为了将高威胁度的安全事件排在所有事件的前面，以便引起安全管理人员的关注，因此安全事件威胁度的划分就显得至关重要。可以通过设计一个匹配器，即将进攻威胁分类情况与安全态势要素提取结果进行匹配，得出结果为高、中、低的安全事件排序情况，直观地呈现给管理人员。

#### 2. 安全态势量化评估模块

安全态势量化评估模块主要完成整个网络当前安全态势的评估，其流程图如图 5-33 所示。安全威胁统计模块针对一定时间段内从安全要素库中提取的安全事件进行威胁度统计分析，得出不同主机服务在不同时间间隔内所受到的高、中、低威胁程度的安全事件数量，并将统计结果提交给服务安全态势评估模块；服务安全态势评估模块依据不同时间间隔的重要性分别计算出对应的服务安全态势，存入态势库中；主机防御措施配置获取模块根据不同主机的安全防御机制，结合对安全属性的要求，计算得到相应主机的防御强度，与主机上的服务安全态势一并提交到主机安全态势评估模块；主机安全态势评估模块依据主机上所运行的服务情况，从权值库中读取其对应服务的权值，估计服务相对于主机的安全影响情况，并将其与该主机的防御强度进行比较便可得该主机的安全态势，存入到态势库中，并提交到网络空间作战态势评估模块；网络空间作战态势评估模块依据各个主机在网络中的不同地位即权值，计算整个网络的安全态势情况，并将结果提交到态势呈现模块把评估结果显示给决策者。

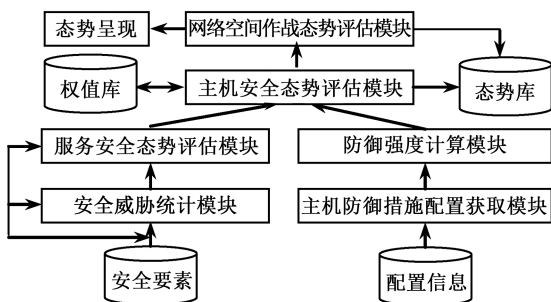


图 5-33 网络空间作战态势量化评估流程图

支持数据库主要有 4 个，分别是安全要素库、配置信息库、权值库和态势库。安全要素库是要素提取层提供的配置信息库；权值库主要负责提供主机上安全防御配置情况，包括时间权值、服务权值、主机权值和安全属性权值，双向箭头表示网络中运行服务和防御机制改变时，权值也要做相应的调整；态势库用于存储服务、主机和网络的安全态势序列，以便为网络空间安全态势动态预测提供必要的数据库支持。

### 3. 安全态势动态预测模块

网络空间作战态势动态预测模块主要完成整个网络空间作战态势的前向预测功能，为此设计了网络空间作战态势动态预测的流程图，如图 5-34 所示。获取模块分别从态势库中读取历史和当前网络空间作战态势数据。历史数据提交给态势预测训练模块用于模型的训练，而当前数据提交给态势预测测试模块用于模型的测试，评价优化模块依据训练和测试评价结果，采用改进遗传算法对小波神经网络预测模型进行优化，直到训练结果满足误差要求，才能确立态势预测模型；态势预测模块将预测结果显示给安全管理人员用于决策分析。

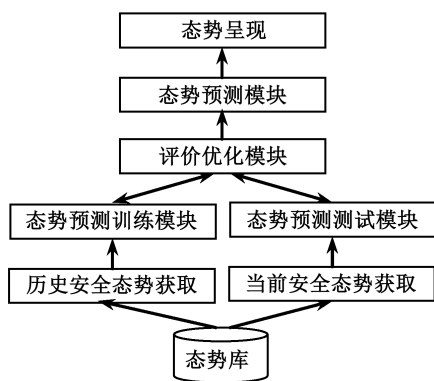


图 5-34 网络空间作战态势动态预测流程图

### 5.6.7 系统部署架构

系统部署架构图如图 5-35 所示，可以部署在传统网络环境中，系统管理员通过监控平台完成对网络空间作战状况的整体感知并采取相应的网络空间安全防护策略，及时有效地处理系统中的威胁，提高系统的安全性。

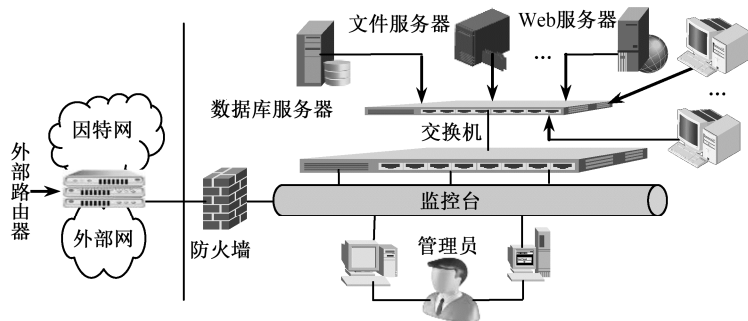


图 5-35 系统部署架构图

系统开发环境的编程语言和相关技术如下：

(1) MyEclipse 开发平台，使用并发版本系统 (CVS, Concurrent Versions System) 进行开发及版本控制；

(2) Oracle 10G 数据库；

(3) PL/SQL Developer 数据库客户端；

(4) Tomcat 应用服务器；

(5) Java 语言、Socket 编程开发后台代码；

(6) SSH (Struts+spring+hibernate) 框架；

(7) ExtJS 框架负责页面展示部分；

(8) FusionCharts、HighCharts 报表控件数据分析展示。

系统是基于 J2EE 技术开发的系统，结合系统功能具体要求可以给出该系统运行时对服务器和客户端计算机配置的最佳要求，具体如下：

(1) 服务器：中央处理器 CPU 主频 2.5GHz 以上；内存 2GB 以上；硬盘最小 160GB 以上；操作系统为 Windows Server 2012。

(2) 客户端：中央处理器 CPU 主频 1.0GHz 以上；内存 512MB 以上；硬盘 80GB 以上；操作系统为 Windows Server 2012, Windows 2010。

## 5.7 网络空间作战态势感知的评估

### 5.7.1 网络空间作战态势感知的评估过程

网络空间作战态势评估是对当前网络状况进行分析并评估。目前网络状况信息，可采用层次分析与模糊匹配结合的算法进行态势评估，态势感知评估流程如图 5-36 所示。各部分功能模块相互协作，完成网络空间作战态势的评估及展示。

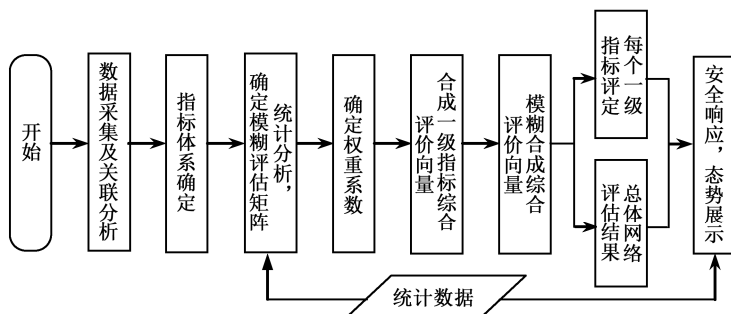


图 5-36 态势感知评估流程

### 步骤一：数据采集及关联分析

通过各种数据采集软件进行数据采集，并进行简单处理，存入基础数据库。

一般需要采集的数据包括：

- (1) 网络流量数据（大小、流量成分信息）。
- (2) 网络性能数据（延迟、抖动）。
- (3) 关键网络设备性能数据（CPU 利用率、端口利用率、路由稳定性数据等）。
- (4) 关键网络设备的配置及漏洞信息。
- (5) 关键网络设施的物理环境信息（温度、湿度、容灾能力）。
- (6) 入侵事件的数量和严重等级。
- (7) 拒绝服务攻击事件的数量和等级。
- (8) 僵尸网络的数量和规模。
- (9) 仿冒及网页挂马网站的数量和分布。
- (10) 垃圾邮件的数量。
- (11) 感染恶意程序的主机数量。
- (12) 安全预警信息（安全通告、安全事件、进攻情报）。

对网络空间作战事件进行关联分析，通过日志和扫描软件获取安全事件，选取合适的阈值，通过数据处理获得安全数据集，对安全事件进行处理。具体算法流程如下：

- (1) 从网络安全基础数据库取出网络安全数据。
- (2) 算法初始值的设定。设置初始阈值、时间初值、相近度的初值。
- (3) 取出给定时间内的网络安全事件数据。
- (4) 循环取出第  $k$  个警报数据，并对安全事件调用相似度计算函数计算初始相似度的值。
- (5) 对计算结果进行比较。如果大于初始值，则更新相近度；如果小于则不变，计数器加 1。
- (6) 初始阈值与相近度进行比较。如果小于阈值则添加报警类别；如果大于阈值则添加新警报。
- (7) 形成网络空间作战数据库。

### 步骤二：指标体系确定

选取指标体系中的分级指标，来进行态势感知体系中一级和二级指标的评价。根据多级评价原则，采用分级评价标准来进行量化处理。

### 步骤三：统计分析，确定模糊评估矩阵

通过对统计的基础数据库和关联分析的安全数据库进行分析形成安全性、脆弱性、可用性、可靠性等基础数据库。通过统计分析形成基础信息的模糊统计矩阵，通过调用基础数据库的数据形成统计矩阵的具体数据，通过分析建立模糊评估矩阵。

### 步骤四：确定权重系数

通过层次分析法进行权重系数的确定。系统实现可通过引入 Java 中的 JAMA（A Java

Matrix Package) 包计算一级判断矩阵的最大特征根并验证是否合理, 并对最后的特征根进行归一化处理。

#### 步骤五：合成一级指标综合评价向量

根据评价向量进行矩阵相乘合成一级指标综合评价向量。

#### 步骤六：每个一级指标的评定

根据步骤五中的合成一级指标综合评价向量及评级标准数据, 进行计算得出每个一级指标的评价标准。

#### 步骤七：总体网络评估结果

根据层次分析与模糊匹配结合评估方法, 采用评估方法中确定的评价算法合成综合评价向量, 再根据每个一级指标的评价结果和评价标准, 并分别对多种评价向量进行综合评价。得出系统态势评估结果。

#### 步骤八：安全响应

根据态势评估结果, 采取相应的响应措施。当系统发生威胁时需要通过自动响应和人工响应两种方式, 并在威胁发生时采用联动响应策略。主要功能包含对关联分析及评估结果的告知功能和网络安全事件发生的响应机制。当系统出现安全威胁时, 系统内部采用一定的响应策略, 同时将威胁信息通过短信或其他形式发送给不同的网络管理员, 这样就形成了联动响应的策略机制, 提高了网络安全管理的效率, 同时也提高了系统的及时响应能力。安全事件的响应流程: 首先是系统根据网络安全态势评估结果采用系统内部响应措施, 然后将系统威胁信息发送至网络安全管理员。通过对响应时间进行分析比对, 采取相应措施并发送, 而联动响应需要通过插件进行调用实现。

#### 步骤九：态势展示

态势展示的主要内容是展示系统作战态势评估结果及网络拓扑结构图中不同网络节点的网络安全状况信息, 以及不同指标下的网络作战态势信息和网络作战告警信息查询等, 从而给作战人员提供决策支持。评估结果包括综合评价结果及分级指标体系的评估结果。网络节点结果主要展示网络拓扑信息及网络节点信息, 主要有设备的详情、风险、报警等信息的展示, 以及简单的网络工具的应用接口。告警信息综合查询主要包括查询网络安全告警信息、历史告警信息、归一化查询字段等。

### 5.7.2 网络态势评估系统体系架构

通过对网络态势感知系统模型的分析, 可以构造出网络态势感知系统评估的体系架构, 其架构图如图 5-37 所示。

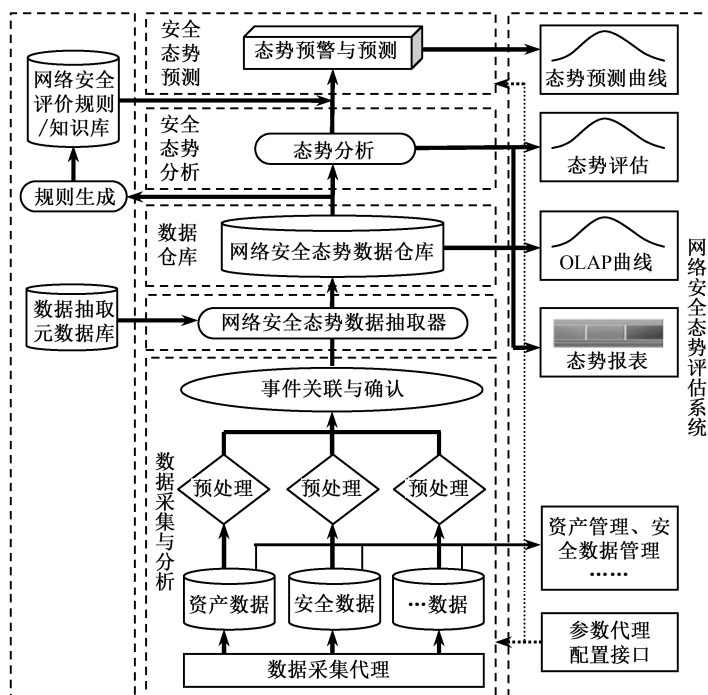


图 5-37 网络态势评估系统体系架构图

该系统自下而上可分为数据采集与分析、数据抽取、数据仓库、安全态势分析、安全态势预警 5 层，其中各层均从下层中获取其处理结果，并向上层提供本层的处理结果。另外，系统提供态势可视化模块，通过各种视图展示态势分析与态势预测结果。在数据仓库的基础上，系统利用数据挖掘技术对网络空间作战态势数据进行数据挖掘，生成态势评估规则，系统利用这些规则，采用各种态势评估模型对网络空间作战态势进行综合评估。最后，系统为用户提供管理接口，使用户能根据自身需求对网络态势感知系统进行动态配置，并对态势分析和预测模型进行修正，实现用户反馈功能。

在网络空间作战态势感知系统中，事件关联与确认、数据仓库、态势分析、态势预测、规则生成是网络态势感知系统的重要组成部分。下面将对以上 5 个模块进行介绍。

### 1. 事件关联与确认模块

作为网络态势感知系统中重要的数据源，IDS 具有告警冗余量大，误报漏报率高的特点，不能直接用于网络空间作战态势分析。在将其装入数据仓库之前，需要对其进行事件关联与确认处理，需要通过引入数据融合、告警聚合等技术来实现。

在数据融合方面，目前用于数据融合领域的典型算法有贝叶斯网络和 DS 证据推理。在告警聚合方面，主要采用聚类与合并、交叉关联、多步进攻关联等技术。聚类与合并过程的主要目的是减少告警数量，采用相似度关联算法以及聚类、分类等算法对原始告警信息进行处理。交叉关联结合背景知识如网络拓扑信息、漏洞信息和主机配置信息等来提高告警的质量。



对于网络态势感知系统,交叉关联更能体现其综合性。多步进攻关联即进攻场景构建,主要研究进攻步骤之间的关联关系。

## 2. 数据仓库

网络态势数据库的构建目的主要有两个方面。一方面,为各种异构的、多源的网络空间作战数据提供一个集成的数据载体;另一方面,数据库中的数据经过数据筛选、数据简约和数据清洗等操作,并根据不同的情况进行数据分析和综合,为下一步的态势分析提供良好的数据基础。

网络态势感知的评估及预测分析都是基于网络态势感知指标体系进行的。因此,网络态势感知数据库的构建也是基于网络态势感知指标体系。指标体系分为一级指标和二级指标。对于每个一级指标,都用一定数量的二级指标来描述其状况,它们共同决定的结果便形成了综合反映网络空间作战态势的网络态势指数,用于参考分析网络当前状况。

从数据库的实施框架来看,首先建立统一的网络态势数据库,该数据库高度集成,访问统一控制。在此统一的标准上根据网络空间作战态势评估的需求,划分不同的数据集市,所有的数据集市从属于数据库,其数据来源也来自数据库。最后根据数据集市分析的性质和面向分析的内容,建立分析主题。

## 3. 态势分析模块

态势分析是指综合大规模网络中各种态势要素,对网络状况进行评估与分析。态势评估的核心是态势评估方法,从态势评估分类来看,大致可以分为3类:基于数学模型的方法、基于知识推理的方法和基于模式识别的方法。基于数学模型的方法就是综合考虑各项态势要素,构造评定函数,建立态势要素集 $R$ 与态势空间 $\theta$ 的映射关系。基于知识推理的方法充分利用经验知识建立态势评估模型,通过逻辑推理判断网络态势完成评估。基于模式识别的方法是指通过机器学习建立态势模版,经过模式匹配,完成对态势的评估。

## 4. 态势预测模块

态势预测在安全事件发生前提前通知网络管理者,并给出安全事件发生时的应急处理方案。对未知和将来可预测的威胁进行有效的管理,即拥有主动防护的能力,为网络管理员制定决策和防御措施提供依据,做到防患于未然。网络态势感知系统应提供对网络威胁进行预测的功能,找出时间序列观测值中的变化规律与趋势,然后通过对这些规律或趋势的外推来确定未来的预测值。态势预测结果最终也要以图形可视化的形式提供给网络管理人员,随着时间的变化,态势预测结果在网络态势图上进行显示。

## 5. 规则生成模块

为了从海量安全态势数据中发现有用的可理解的安全事件模式和安全评估规则,实现对安全行为特征的分析 and 抽取,可利用以下几种数据挖掘技术:

(1) 关联规则技术。利用关联规则,分析网络空间安全行为与各个属性特征之间的相

关度。不安全的行为会导致网络空间安全防护出现隐患，通过发现各个不安全行为特征值，推导出威胁网络空间安全的相关行为、动作，由此产生关联规则，建立这种规则上的知识库可形成实时、准确和有效的推理机制。

(2) 孤立点事件分析。孤立点事件主要是基于偏离的孤立点检测在异常检测中的运用。

(3) 分类技术。网络空间作战检测中涉及海量的数据分析，其中包括网络日志记录分析、临时文件分析、路由器工作日志分析等。通过收集丰富的“正常”或“异常”的安全行为数据，利用分类算法学习得到的分类器来标志或预测新的网络空间安全行为。

(4) 聚类技术。典型的聚类规则是通过某主机网络日志的数据传输记录，可通过聚类分析得出该主机使用者的网络使用习惯甚至推理出该用户的兴趣、爱好，确定它在网络空间作战检测和防御中占据的地位。

(5) 序列分析技术。威胁网络的各种不安全行为在各时间点上发生的事件以及各独立事件间的顺序上有一定的规律。通过研究模式挖掘算法，从海量数据中挖掘出黑客的进攻模式。

5.7.3 态势评价指标选取

合理的评价体系能够使决策者更容易、更快速地了解当前网络的状况，以便做出决策。网络空间作战态势评价指标的选取原则：

- (1) 相似相近原则，要统一考虑对网络产生影响的相似、相近、相互影响的因素。
- (2) 分层原则，按照数据的特点和来源，结合网络的范围大小进行分层处理。
- (3) 动静结合原则，动态的流量数据等与相对静态的网络拓扑结构数据应区别对待，静态的指标在一定时间内是保持不变的，而动态的会随时改变，处理起来需要使用不同的方法进行区别对待。

结合上述评价指标的选取原则，可将态势评价指标分为一级、二级和三级指标。其中，一级指标包括五大类别，即基础运行、网络脆弱性、网络威胁、网络稳定和作战态势提取指标。网络空间作战态势评估指标体系见表 5-3。

表 5-3 网络空间作战态势评估指标体系

一级指标	二级指标	三级指标
基础运行指标	网元信息	主机数量
		不同端口对应的主机数量
		主机操作系统与版本
		不同服务对应的主机数量
	基础流量指数	流量规模指数
		传输质量指数（延迟、抖动）
		带宽使用率

续表

一级指标	二级指标	三级指标
基础运行指标	设备负载指数	核心路由器负载
		核心交换机负载
		DNS 服务器负载
	物理环境运行指数	温度指数
		湿度指数
网络脆弱性指标	关键设备健康指数	DNS 服务器健康指数
		核心路由器健康指数
		核心交换机负载
		关键业务服务器负载
		主机健康指数
	服务器主机健康指数	服务器配置合规率
		服务器软件更新率
	终端主机健康指数	终端主机配置合规率
		终端主机软件更新率
	关键网络设施健壮指数 (容灾能力)	关键设备访问主流安全网站的频率
		服务器线程数
	漏洞指数	网络漏洞数目及等级
		关键设备漏洞数目及等级
	子网内软硬件指数	子网内安全设备数目
		子网内各主机提供的服务种类及其版本
		子网内各主机的操作系统类型及其版本
		子网内各主机开放端口的总量
	静态配置信息指数	网络拓扑指数
		防护软件安装情况
		子网内安全设备数目
网络威胁指标	进攻烈度指数	入侵事件指数
		DDoS 事件指数
		僵尸活跃度指数
	网络欺诈频度指数	网页挂马密度指数
		仿冒网站密度指数
	网络风险指数	垃圾邮件泛滥指数
		病毒流行指数
	报警数目	木马攻击
		DoS 攻击
		病毒攻击
		蠕虫攻击
		各类攻击发生频率
		各类安全日志信息
	安全预警指数	漏洞发现

续表

一级指标	二级指标	三级指标
网络威胁指标	安全预警指数	病毒流行的安全通告
		各类攻击预告
	子网使用指数	子网带宽使用率
		子网内安全事件发生频率
		子网内各主机提供的服务种类及其版本
		子网数据流入量
	子网数据流量指数	子网流入量增长率
		子网内不同协议数据包的分布
		子网内不同大小数据包的分布
		流入子网内数据包源 IP 分布
网络稳定指标	子网存活指数	流出子网数据包目的 IP 分布
		子网内主机平均存活时间
		子网内存活主机数目
		子网平均无故障时间
	子网数据流变化率指数	子网流量变化率
		子网内不同协议数据包分布比值的变化率
		子网内不同大小数据包分布比值的变化率
		子网数据流总量及变化率
		CPU 占用率
		平均 IP 数据报传送时延
作战态势提取指标	数据报传送性能评估指标	IP 数据报时延变化
		IP 数据报差错率
		IP 数据报丢失率
		IP 数据报严重丢失块比
		数据报统计流量
	数据报统计信息评估指标	请求报比率
		响应报比率
		端口利用率
		平均输入速率
		平均输出速率
		平均吞吐率
	数据报检测信息评估指标	报文类型状况
		报文长度状况
		报文载荷状况
		端口流量状况

(1) 基础运行指标。这是表征当前网络性能、传输设备负载、物理环境的一系列指标。尽管这些指标不直接反应安全问题，但是作为基础运行态势，会对安全态势起到间接的影响。例如，如果网络的基础流量很大，一旦有大流量的进攻发生时，网络就很容易拥塞。

基础流量直接影响着网络的抗冲击能力。

(2) 网络脆弱性指标。该指标表征的是网络整体上漏洞和脆弱性的情况,指被监控网络在相同的进攻环境中易于遭受进攻的程度。可以根据网络的性质和规模数据采集的可行性等因素的不同,对脆弱性指标的内涵也不同。例如,对于一个大型的企业网,关键业务服务器是企业自身的业务服务器。如果网络环境是城域网,关键业务服务器就应该是可以影响社会稳定、关系国计民生的网络服务器,如网络银行服务器、各种在线支付服务器、大型电子商务网站服务器、各种电子政务服务器等。

(3) 网络威胁指标。该指标表征的是网络上各种威胁因素的情况,指在监控对象网络内部条件不变的情况下,各种网络活动对于网络内部可能产生的威胁的程度以及危害的严重性。威胁的情况主要包括各种网络进攻的发生的频率和规模、各种潜在的威胁手段。

(4) 网络稳定指标。它指被监控对象自身状况是否变化及其变化的程度。

(5) 作战态势提取指标。该指标包括数据报传送性能、统计信息和检测信息的评估指标。

## 5.8 网络空间作战态势感知的预警

尽管防火墙、入侵检测系统等安全部件被部署到重要的网络空间应用系统中,但是,这些技术和系统都是要等到攻击发生了,才能有所反应。应该运用预警技术监控和识别受保护网络上的入侵企图和入侵行为,把控网络风险,在入侵发生或入侵造成严重后果前,预先采取相应的防御措施来加强网络的安全。

### 5.8.1 概念与目的

网络空间作战态势感知的预警是指对分布于网络空间上不同网段的入侵检测传感器所采集的信息数据进行有效、合理的监视、识别和分析,从中提取网络空间态势信息,发现入侵倾向和潜在的或可能的威胁,从而准确地判断网络中的攻击意图,发出预警,预测潜在的、未来的目标或攻击的发展方向的一种技术。

面对无孔不入、无时不在的网络入侵攻击,构建一个相对完备的网络空间安全预警系统,至少应实现以下多层次目标:

(1) 对网络基础设施的安全状况及威胁的来源和程度能迅速全面系统地做出风险评估。

(2) 以网络入侵威胁来源为对象,按时间顺序、入侵序列、动作意图、威胁范围和程度能实时地进行统计、分析及审计。

(3) 对来自外部网络的恶意代码和违规操作能快速地通过入侵事件归约、融合关联分析进行识别、跟踪、记录、分类和报警，提高系统及时、主动发现入侵攻击事件的能力。

(4) 建立一套有效的“预警响应”运行机制，为遭到破坏的网络及信息系统的恢复提供技术性支持，任何时候都不能区分闲时、忙时而松懈和疏忽，不能有平战转换的结合部和过渡期，做到平时与战时无缝衔接，使网络态势预警管理无懈可击。

## 5.8.2 预警系统的组成

态势感知预警系统由四个相互关联的子系统组成，如图 5-38 所示，包括识别子系统、评估子系统、预警子系统和响应子系统。这四个子系统涵盖了从确定警情指标、寻找警源、分析警兆、准确及时报警，确定警情应对措施以及排除警情并收集反馈信息的全过程。

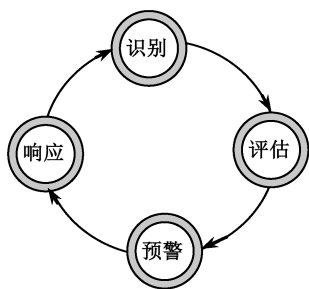


图 5-38 预警系统组成图

这四个子系统的作用可以概括为：识别即监视警源、发现警兆；评估即预测警情、判定警损；预警即提出警示、选择对策；响应即排除警险、消除隐患。

识别子系统利用各种网络态势感知工具收集受监控网段的作战态势相关数据，包括网络数据、流量数据、系统日志、攻击警报等，并形成相关的信息报告提交给评估子系统。

评估子系统利用数据融合等技术手段，对识别子系统提交的信息报告进行评估，形成关于全网态势的评估结果提交给预警子系统。

预警子系统根据评估结果，利用建立好的数据模型，对可能存在的攻击做出预测，发现系统中存在的问题，并给予报警警示。

响应子系统则负责采取各种技术手段，限制攻击的扩散，消除攻击的影响。

## 5.8.3 预警系统的结构

网络态势感知预警系统采用分布式体系结构，主要由检测域、预警代理、区域预警中心这三部分组成。检测域包括多个网段，其中包含若干个预警代理，主要进行数据包获取、预处理和检测分析。预警代理由分布在不同网段的网络检测机制组成。区域预警中心对报警信息进行数据融合分析。

### 1. 检测域

网络态势预警系统把要保护的网段划分为不同的检测域，每个检测域包含若干个网段。

在检测域确定后,其所包含网络的主机 IP 地址也确定了,从而检测域可以与主机 IP 地址范围进行绑定。检测域中包含主机、交换机、路由器、防护墙和各种应用服务器等。在检测域中,还加入了两大安全组件——预警代理和区域预警中心从事报警信息分析和响应。

## 2. 预警代理

预警代理模块如图 5-39 所示,在每个网段中都有一个预警代理,它负责对本网段数据的获取、预处理和检测分析。经过检测分析后把报警信息传送到区域预警中心。将数据检测分析放在预警代理而不是放在区域预警中心,因为这样可以减少网络数据传送到区域预警中所带来的网络开销,平衡各个检测域的数据检测效率,从而提高实时性和并行性。

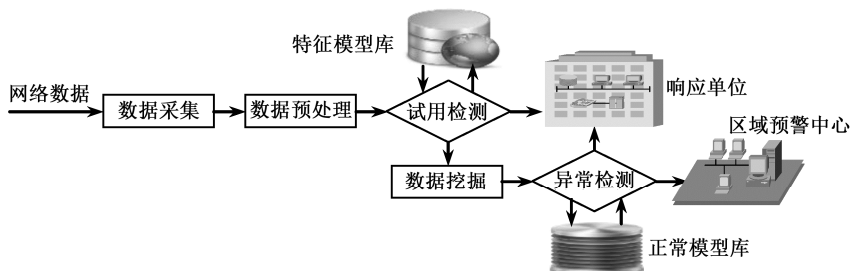


图 5-39 预警代理模块

数据的获取可以通过将网卡设置为混杂模式的方式得到。对捕获的数据包先进行预处理,将数据转换为相应的数据处理格式,然后进行检测分析。

## 3. 区域预警中心

区域预警中心对预警代理传送的报警数据先进行冗余归并,然后进行数据融合分析,发现事物之间的因果联系,实现报警关联。预测网络可能遭受的攻击和对本区域的网络进行威胁评测,对攻击行为进行响应并向检测域发送预警信息。区域预警中心的设计如图 5-40 所示。

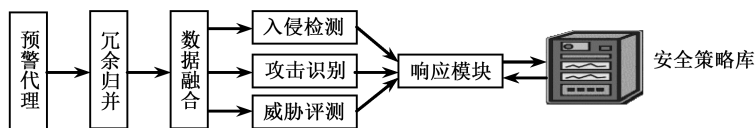


图 5-40 区域预警中心的设计

区域预警中心对本检测域的所有预警代理传送的报警信息进行检测分析,同时结合本地知识库进行数据融合分析。每个区域预警中心都有一张检测域和其对应的主机 IP 地址映射表。如果区域预警中心产生预警,则根据检测到威胁数据的检测域与 IP 地址的映射表,将报警信息发送到相应的检测域。

区域预警中心是网络安全预警系统的核心模块,它的主要功能是对报警信息进行冗余归并、信息关联融合、攻击识别、威胁评测和信息控制管理。

#### 5.8.4 预警系统的工作流程

图 5-41 给出了网络态势预警系统的工作流程图。首先由检测域采集处理网络数据包,然后将报警信息数据发送到预警代理,对其进行误用检测和异常检测,再经过区域预警中心的冗余归并和关联融合后将确定的入侵事件发送给控制响应模块进行处理,而异常信息根据融合结果进行攻击识别、威胁评测和更新入侵特征,并把报警信息发送给控制响应模块。控制响应模块负责更新入侵模式库和过滤规则库等。

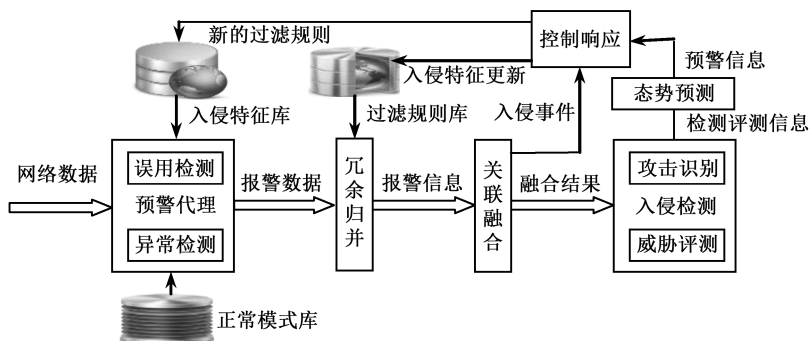


图 5-41 网络态势预警系统工作流程图

经过误用检测和异常检测,把可疑事件和入侵信息发送到区域预警中心,区域预警中心对报警信息进行冗余归并、数据融合,预测当前网络或未来网络可能发生的攻击和进行网络威胁评估,对入侵行为采取一定的安全策略,如发出警报、切断网络等。

报警信息冗余归并把预警代理模块传送的报警信息先进行初步处理,使具有明显特征且具有很高响应优先级的报警信息及时响应。

信息关联融合处理是对报警信息在冗余归并后的进一步分析,即报警关联分析和数据融合。对数据融合分析的三种结果(入侵、异常、正常)采取相应的分析响应模式:对于入侵信息直接发送至控制响应模块,并由控制响应模块向检测域发送预警信息;对于异常信息发送至攻击识别模块,根据攻击预测结果识别入侵行为,并由控制响应模块向对应的检测域发送报警信息;对于正常信息,则忽略本次报警信息。

网络攻击识别对预警代理检测后的报警信息,经过冗余归并和数据融合处理,预测未来网络可能遭受的攻击,发出预警信息。

网络威胁评测主要通过检测设备进行检测和用人工系统进行测试、分析和评估数据。在评估的过程中，自然对正常的数据和伪数据进行过滤和删除，重要的数据信息才会提交给预警系统。检测设备主要有异常流量监测设备、入侵检测/防护设备、Web 应用防火墙、网络防病毒设备、威胁分析系统等。评估采用静态评估和动态评估两种。静态评估针对网络系统中的所有因素，是对其潜在的威胁进行评估，不考虑运行时的外界因素，主要是从管理和技术两个方面来进行的；而动态评估则是考虑网络运行时的所有因素，实时测量和评估网络系统的状态。



态势预测会根据入侵检测、识别和评测的信息，并结合历史态势情况对可能出现的攻击预测正在发生和将要发生的风险。

控制响应会根据预警信息提交给报警，给予报警警示。另外，控制响应会根据入侵特征更新过滤规则库；并根据新的过滤规则更新入侵特征库。

信息控制管理对上传来的报警信息进行存储和管理，并建立相关入侵行为的知识库，主要功能是描述当前的网络安全状况、攻击者的攻击历史等，为攻击识别和威胁评测提供依据。

### 5.8.5 态势预测子系统功能描述

态势预测子系统主要负责挖掘网络历史态势数据的变化规律及其发展趋势，从而预测出网络态势未来的发展变化，为管理员及时了解网络状态，制定安全策略提供依据。

预测模型会根据用户的需要自动生成，在用户输入预测对象、预测强度及预测精度后，系统会自动确定输入指标的类型，历史数据调用的多少以及所预测时间范围的大小。如果用户的需求改变则可以更改模型配置参数，生成新的预测模型，以达到最理想的预测效果。

在预测模型生成以后，系统会根据模型需要自动调用相应数据进行预测。由于模型中包含多种预测算法，因而会产生多个预测数据。为了能取得最好的预测效果，系统将根据各算法产生结果的历史准确率，对该组数据进行加权平均计算，综合得出最理想的结果，作为最终的预测数据输出。

同时，预测子系统还具有自适应的功能，每次态势评估子系统计算出的态势值都将作为训练数据输入预测模型的权值调整模块中，从而不断调整模型各参数权重，以适应当前网络状况。另一方面，预测数据与真实数据的比较也会得出相应预测算法的准确率，该数据将会作为训练数据输入预测结果修正模块中，不断调整各个权值，从而获得最理想的预测效果，其数据流图如图 5-42 所示。

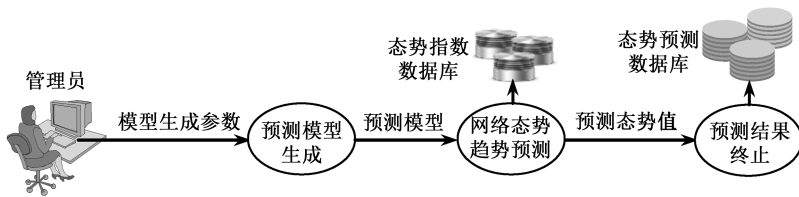


图 5-42 态势预测子系统数据流图

#### 1. 模型初始化

该部分主要负责预测模型训练前的初始化工作。影响系统预测效率及精度的因素主要包括三个方面：预测周期、预测强度和样本数量。其中，预测周期和预测强度决定了预测过程中数据间的映射关系，即由前  $M$  个数据预测后  $N$  个数据。而样本数量则决定了调用

历史数据的多少。模块为用户提供配置接口，用户可根据自身需要，选择适当的参数以达到相应的预测要求，若用户没有进行配置则采用系统默认配置。参数选定后，系统从数据库中读取相应的样本集，然后将其转化为一系列  $M$  元组向量，为下一步的模型训练生成做好准备。模型初始化数据流图如图 5-43 所示。

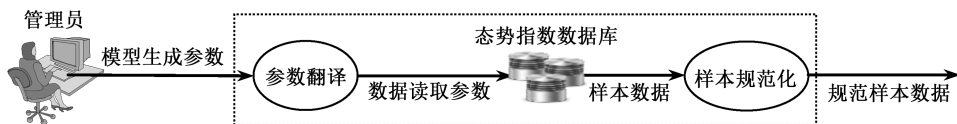


图 5-43 模型初始化数据流图

## 2. 预测模型生成

该部分主要负责预测模型的训练生成。初始化过程结束之后，系统开始训练样本数据，以从中分析其发展变化规律，进而寻找出时间序列中前  $M$  个态势值与随后  $N$  个态势值间的映射关系，并由此拟合出关于时间的网络空间作战态势值函数，即生成网络态势预测模型。预测模型生成模块数据流图如图 5-44 所示。

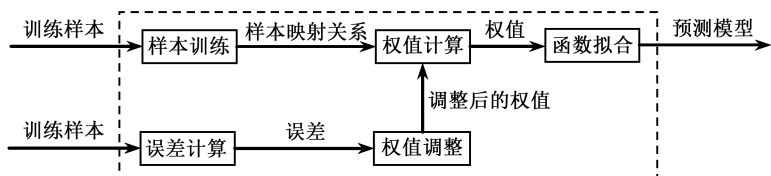


图 5-44 预测模型生成模块数据流图

## 3. 趋势预测

该部分主要负责对网络态势未来发展趋势进行分析并预测。在预测出未来时间段的网络态势值后，它与历史态势值组成了一个新的时间序列。通过分析计算该序列的各类统计特征，如趋势特征和周期特征，使用户能更直观地了解网络发展的趋势，为可能发生的网络空间安全事件提前做好防御准备。网络态势趋势预测数据流图如图 5-45 所示。

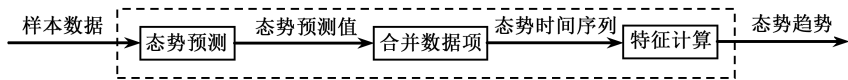


图 5-45 网络态势趋势预测数据流图

## 4. 态势预测方法介绍

态势预测的方法主要有：

(1) 非模型预测法，是指预测者依靠熟悉业务知识、具有丰富经验和综合分析能力的人员与专家，根据已掌握的历史资料和直观材料，运用个人的经验和分析判断能力，对事

物的未来发展做出性质和程度上的判断,然后,再通过一定形式综合各方面的意见,作为预测未来的主要依据。主要包括专家预测法、德尔菲法、个人判断法、头脑风暴法、相关类推法、对比类推法、比例类推法、指标预测法、情景预测法和主观概率预测等法。

(2) 因果分析预测法,是以因果性预测原理做指导,以分析预测目标同其他相关事件及现象之间的因果关系,对未来状态与发展趋势做出预测的分析方法。主要有回归分析预测法、统计计量模型预测法、投入产出分析预测法和灰色系统模型预测法。

(3) 时间序列预测方法,就是通过编制和分析时间序列,根据时间序列所反映出来的发展过程、方向和趋势,分析它随时间的变化趋势,并建立数学模型以预测目标未来可能达到的水平的预测方法。主要有简单序时平均数法、加权序时平均数法、移动平均法、加权移动平均法、自回归滑动平均模型法、趋势外推法、指数平滑法、时间序列分解法、季节性趋势预测法和马尔可夫时序预测法等。





# 第 6 章

## 进攻性网络空间作战

进攻性网络空间作战是指在网络空间作战中利用敌方网络系统自身存在的安全漏洞、隐患或缺陷，通过使用网络作战命令和专用软、硬件工具进入敌方网络系统，获取、修改、伪造、破坏或删除敌方网络系统中的信息以及添加无用或有害信息，中断、拒绝、降级、破坏和操纵敌方网络系统，或者使用强电磁武器摧毁其硬件设施而采取的一系列作战措施和行动的总称。在未来战争中正确地组织与实施网络进攻去夺取战场制网络权，是夺取战场制信息权进而赢得战争胜利的重要行动。

### 6.1 概述

#### ■ 6.1.1 进攻性网络空间作战的目的

进攻性网络空间作战就是要夺取和控制网络权、瘫痪敌实体作战力量、削弱敌战争潜力、进行网络侵扰，以及破坏敌信息资源的可用性、机密性和完整性。所以，从进攻者角度来看，其进攻行为要实现的目标也就是这七个方面。

(1) 以夺取和控制网络权为目的。实施网络空间进攻作战,应以争取制网络权为目的。首先以敌网络空间感知系统为目标,对其实施攻击,使敌无法及时、准确、全面地掌握网络空间态势;其次以网络空间武器为目标,阻碍其正常运行,削弱敌反击能力;再次就是利用互联网对敌方国家施加政治、文化影响,并在必要时通过网络控制敌方国家的关键基础设施。如果在作战中保持了制网络权,就意味着具有强大的战斗力;如果丧失了制网络权,即使己方人员、装备完好无损,也仍然是一盘散沙,形不成战斗力。未来战场,谁在作战中控制网络的能力更强、更持久,谁就将夺取战争的胜利。

(2) 以瘫痪敌实体作战力量为目的。主要是对其网络空间中的侦察监视、指挥控制、交战网络系统实施进攻,通过破坏网络来瘫痪敌网络所控制的经济、军事指挥控制系统,使敌实体作战力量失去网络空间的支持和对网络空间的开发利用。手段包括网络病毒、电磁脉冲武器等。

(3) 以削弱敌战争潜力为目的。应通过网络空间对敌各个行业、各个产业的网络系统实施攻击,干扰、瘫痪、破坏其工业、金融、社会系统等的正常运行,在造成、引起敌方混乱的同时,积极激发群体事件,削弱政府控制能力,削弱其军事功能的发挥。

(4) 以网络侵扰为目的。侵入敌方网络窃取机密情报,对敌人的雷达、通信等信息系统进行破坏。

(5) 以破坏敌信息资源的可用性为目的。使敌使用信息资源的要求无法实现。在网络环境中,拒绝服务攻击、部分计算机病毒攻击和蠕虫攻击都可以实施对信息可用性的攻击。

(6) 以破坏敌信息资源的机密性为目的。指进攻者获取超出其权限以外的信息资源或系统资源。最常见的窃听、口令攻击就是攻击信息的机密性。另外,木马攻击和部分蠕虫攻击也可以窃取并泄露信息系统的机密性。还有一种更隐蔽的攻击方式,即通信量分析,它可以通过获取通信双方的身份、通信密度等信息而破坏通信的机密性。

(7) 以破坏敌信息资源的完整性为目的。在这里,信息的完整性是信息的正确性和一致性的综合。攻击行为就是在信息的存储或传输过程中对信息进行更改和破坏,也包括“虚假”信息的注入和失效信息的“重放”。常见的“中间人”攻击就是攻击信息完整性的一种典型方式,它还可以结合一些其他的攻击手段,如IP欺骗、DNS欺骗等,实现对信息的可用性、机密性和完整性这三个方面的攻击。

## 6.1.2 网络空间进攻作战的原则

### 1. 军民融合,全民皆兵,组织具有人民战争特色的进攻力量

网络空间进攻作战,应贯彻“军民融合”原则,加强对民用通信、邮电、能源等网络空间设施的军事化开发利用,确保必要时直接投入作战;动员和使用地方雄厚的网络技术人才参战作战,壮大网络空间进攻作战力量。应贯彻“全民皆兵”原则,利用许多国家和

地区军网、民网互联融合，网络资源普遍共享，特别是可用作网络进攻武器的资源容易获取、简便易行的状况，以及网络空间攻击行动发起门槛较低，国家、军队、非政府组织甚至个人都有能力发起攻击行动的情况，充分发动网络空间中的众多用户，组织成为我方的作战力量，对敌发动网络空间“人民战争”。

## 2. 攻防兼备，奇正结合，确立以攻求奇的进攻原则

网络空间进攻作战应在攻防兼备的基础上实施。进攻和防御是作战行动中不可分割的两个部分，通过防御，可以最大限度地降低敌对我方网络系统的毁伤程度，使我方网络空间进攻能力得以保持；有效的进攻可以从根本上削弱甚至摧毁敌方的网络空间作战能力，降低我方的防御压力。

《孙子兵法》强调“奇正”，“战势不过奇正，奇正之变不可胜穷也”“凡战者，以正合，以奇胜”。而网络空间具有物理分布的立体性、体系结构的层次性、拓扑结构的动态性、共享资源的丰富性、应用功能的多样性，以及涉及领域、活动角色的多元性等特点，为网络空间进攻作战确立“奇正结合”“以攻求奇”原则，实现“以奇胜”提供了广阔的物理空间和逻辑层次、丰富的利用资源、多样且强大的实施手段、多元的目标选择和力量编组。

## 3. 平战一致，多法并举，实施全面综合的进攻行动

实施网络空间进攻作战，应贯彻“平战一致”原则。一是平时有针对性地研究入侵武器和方法，适时进入敌网络并潜伏其中，战时则根据需要适时发起攻击。二是一些对抗方式、方法在平时战时都在使用，如黑掉网站、阻塞通信、设置后门等。三是各类角色平时战时都在网络空间中开展活动，或由于政治事件、地区冲突，对政府网站、金融机构实施网络攻击；或出于战略安全考虑，对敌重要基础设施设备实施网络攻击。应贯彻“多法并举”原则，或安置“逻辑炸弹”，适时启动破坏敌方信息系统数据；或伪造数据获取合法身份和权限，侵入敌方网络空间；或通过间谍渗入敌内部，对其网络系统植入病毒。应实施全面综合的进攻行动：一是在陆、海、空、天、电领域，围绕网络空间信息流动、软硬件生产的整个流程实施攻击行动；二是既发挥技术的基础作用，以技术推动战术，又发挥战术的能动作用，以巧妙的战术弥补技术差距。

## 4. 网络中心，软硬兼顾，发挥软件主战的进攻作用

网络空间进攻作战，应贯彻“网络中心”原则，树立以网络空间为中心的观念，即以网络空间为主战场，主要利用网络空间中的资源作战，主要针对网络空间中的目标作战，主要通过对网络空间的控制达成对网外空间的政治、军事、社会、金融、工业、商业等领域的强有力的影响。应当“软硬兼顾”，既要针对软件目标，包括各类信息系统、数据库系统，也要针对硬件目标，包括支持网络空间的各类网络设施设备，以及网络系统控制下的各类硬件；既要采取软的手段实施软杀伤，主要以病毒、木马、分布式攻击等，干扰、压制、削弱敌网络空间各系统的功能，也要采取硬的手段实施硬摧毁，主要以常规火力打击、特战人员破袭、电磁脉冲攻击等，摧毁、破坏敌网络空间各系统，以及杀伤敌网络空

间作战人员等。在“软硬兼顾”的基础上，应注重发挥软件主战的进攻作用。因为，数据处理、人工智能、虚拟现实、作战指挥软件等都是作战系统的重点，是实现从数据优势到认知优势，再到行动优势的关键所在；侦察监视、指挥控制、打击评估过程很大程度上取决于相应软件系统的运行状况；有的软件系统被专门设计为攻击性武器，如“震网”，所以应充分认识并发挥软件主战的进攻作用。

### 6.1.3 进攻性网络空间作战的分类

#### 1. 网络空间进攻分类的基本原则

网络空间进攻分类体系应该具备的原则主要有：

- (1) 可接受性：分类方法符合逻辑和惯例，易于被大多数人接受；
- (2) 确定性（也称无二义性）：对每一分类的特点描述准确；
- (3) 完备性（也称无遗漏性）：分类体系能够包含所有的攻击；
- (4) 互斥性：各类别之间没有交叉和覆盖现象；
- (5) 可重现性：不同人根据同一原则重复分类的过程，得出的分类结果是一致的；
- (6) 可用性：分类对不同领域的应用具有实用价值；
- (7) 适应性：可适应于多个不同的应用要求；
- (8) 原子性：每个分类无法再进一步细分。

另外，还有一些非主流的原则，如攻击分类方法应当是客观的、可理解的、稳定的，所使用的技术术语应当具有准确的定义，对内部攻击和外部攻击应该加以区分等。

#### 2. 网络空间进攻分类方法

目前，已有的网络空间进攻分类方法大致可以分为下面几类。

##### 1) 按经验术语分类

按经验术语分类是指利用网络空间进攻中常见的技术术语、社会术语等来对攻击进行描述的方法。这类攻击主要有病毒和蠕虫、资料欺骗、拒绝服务、非授权资料拷贝、侵扰、软件盗版、特洛伊木马、隐蔽信道、搭线窃听、会话劫持、IP 欺骗、口令窃听、越权访问、扫描、逻辑炸弹、陷门攻击、隧道、伪装、电磁泄漏、服务干扰、伪造网络资料、冒充他人、网络探测、电子邮件溢出、时间炸弹、获取工作资格、刺探保护措施、干扰网络、社会活动、贿赂、潜入、煽动等。

##### 2) 按单一属性分类

按单一属性分类是指仅从攻击某个特定的属性对攻击进行描述的方法。从系统滥用的角度将攻击分为 9 类，即外部滥用、硬件滥用、伪造、有害代码、绕过认证或授权、主动



滥用、被动滥用、恶意滥用、间接滥用。依据攻击实施的手段进行分类，可归纳为 5 种，分别是中断、拦截、窃听、篡改、伪造。从进攻的实施方法将网络空间进攻分成物理攻击、系统弱点攻击、恶意程序攻击、权限攻击和面向通信过程的攻击这 5 类。依据攻击后果分成窃取口令、错误和后门、信息泄露、协议失效、认证失效、拒绝服务等类别。

3) 按多属性分类

按多属性分类是指同时抽取攻击的多个属性，并利用这些属性组成的序列来表示一个攻击过程，或由多个属性组成的结构来表示攻击，并对过程或结构进行分类的方法。

按多属性分类的出发点是将一个攻击看成一个由多个不同阶段组成的过程，而不是一个单一的阶段，其中不同的阶段体现出不同的攻击特点。具体的分类对攻击的 7 个属性进行了描述，具体包括：攻击者类型、所使用工具、弱点、攻击行动、攻击目标、未授权访问和攻击目的，如图 6-1 所示。

攻击者类型	所使用工具	弱点	攻击行动	攻击目标	未授权访问	攻击目的
黑客	物理攻击	设计	探测	账户	越权访问	热衷挑战
间谍	信息交换	实现	扫描	进程	信息泄露	政治利益
恐怖分子	用户命令	配置	泛洪	数据	信息损毁	经济利益
集体入侵者	程序脚本		认证	组件	拒绝服务	蓄意破坏
职业犯罪	自治代理		绕过	计算机	资源窃取	
故意破坏者	工具箱		欺骗	网络		
刺探隐密者	分布式工具		读取	互联网		
	数据窃听		复制			
			窃取			
			篡改			
			删除			

图 6-1 基于多属性的攻击分类

基于多重属性的分类法能比较全面地刻画攻击特征，通过组合及增加属性值能将新型攻击纳入分类体系，可扩展性较好，适用范围较广。

4) 按攻击手法分类

按攻击的手法分为读取攻击、操纵攻击、欺骗攻击、泛洪攻击、重定向攻击、拒绝服务（DoS）攻击、Web 攻击、病毒型攻击和混合攻击。

（1）读取攻击是指在未授权情况下查看信息的攻击。这类攻击主要有嗅探攻击、侦察攻击、口令猜测、会话劫持、利用信息服务和直接进入攻击等。其中，侦察攻击又包含数据整理攻击、拨号式扫描/移位式扫描攻击、探测/扫描攻击。利用信息服务又包括 DNS 域转换、Finger 服务、轻量级目录访问协议（LDAP，Lightweight Directory Access Protocol）服务。扫描技术又有地址扫描、端口扫描、漏洞扫描、反响映射和慢速扫描。

(2) 操纵攻击是指修改网上信息的攻击。这类攻击主要有网络操纵攻击和应用程序操纵攻击等。其中，后者又包括缓冲区溢出攻击和 Web 应用程序攻击。

(3) 欺骗攻击是指提供虚假信息或虚假服务的攻击。这类攻击主要有 MAC 欺骗攻击、源 IP 地址欺骗攻击、源路由欺骗攻击、传输欺骗攻击、身份欺骗攻击、DNS 高速缓存污染、伪造电子邮件和无赖设备攻击等。其中，传输欺骗攻击又包括 TCP 欺骗攻击和 UDP 欺骗攻击。

(4) 泛洪攻击是指使计算机资源发生溢出的攻击。这类攻击主要有 MAC 泛洪攻击、TCP SYN (synchronous) 泛洪攻击、网络泛洪攻击和应用程序泛洪攻击等。

(5) 重定向攻击是指更改后续信息的攻击。这类攻击主要有端口重定向、IP 重定向攻击、L2 重定向攻击和传输重定向攻击等。L2 重定向攻击又包括 ARP 重定向/ARP 欺骗攻击和生成树协议 (STP, Spanning Tree Protocol) 重定向攻击。

(6) 拒绝服务 (DoS) 攻击是指通过使服务计算机崩溃或把它压垮来阻止提供服务的攻击行为。常见的 DoS 攻击方式有死亡之 Ping、泪滴、UDP 洪水、SYN 洪水、Land 攻击、Ping 洪流、Rwhod、Smurf 攻击、Fraggle 攻击、电子邮件炸弹、畸形消息攻击和 DDoS 攻击等。有两类最常见的 DDoS 攻击，即资源耗尽型和导致异常型攻击。

(7) Web 攻击主要阻碍合法用户对站点的访问，降低其可靠性。主要攻击方式有 SQL 注入攻击、跨站脚本攻击、网页挂马、信息泄露、网页木马、僵尸网络、网络蠕虫、目录遍历攻击、操作系统命令注入攻击、社会工程学攻击和 Script/ActiveX 攻击等。

(8) 病毒型攻击是指利用病毒对网络空间实施的攻击行为。主要有利用伴随型病毒、源码型病毒、嵌入型病毒、外壳型病毒、寄生型病毒、诡秘型病毒、变型病毒 (又称幽灵病毒)、引导区病毒、文件型病毒、复合型病毒、“蠕虫”型病毒、宏病毒、特洛伊木马、操作系统型病毒等进行的攻击。

(9) 混合攻击采用不止一种所列的方法的攻击。这类攻击主要有中间人攻击、Rootkit、远程控制软件攻击、病毒/蠕虫/特洛伊木马等混合情况下的攻击。

#### 5) 其他网络空间进攻分类

(1) 从发生背景上，可分为武装冲突背景之下的网络进攻和平时时期条件下的网络进攻。

(2) 从进攻规模上，可分为零星的、小规模的网络空间进攻和有组织的、大规模的、破坏性强网络空间进攻。

(3) 从进攻目标上，可分为针对国家政府系统的网络进攻和针对私人主体的网络进攻。

(4) 从作战手段上，可分为网络盗窃战、网络舆论战、网络摧毁战的网络进攻。

(5) 从攻击地位上，可分为主动出击式进攻和被动防御式进攻。

(6) 从攻击方法上，可分为基于网络协议的进攻和基于系统安全漏洞的进攻。

(7) 从攻击违反国际法的严重程度,可分为未达到非法干涉的、达到干涉但未达到使用武力的、达到使用武力但未达到武装冲突的和达到武装冲突的网络空间进攻。

### 6.1.4 网络空间进攻的流程

#### 1. 一般进攻过程

网络空间进攻的一般过程为:首先隐藏己方(进攻方)的位置,然后通过各种方式对要攻击的敌方目标网络系统的信息进行收集;在收集到的信息的基础上进行各种漏洞和脆弱性分析,找出可以利用的漏洞然后利用漏洞进行攻击。在攻击过程中,一般先获得敌方系统一定的权限,如普通用户的访问权限,对系统文件的读、写等权限;然后再根据攻击的目的进行攻击;最后留下后门,清除痕迹。其过程如图 6-2 所示。

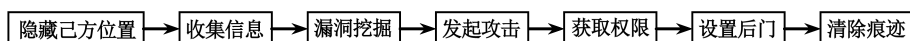


图 6-2 网络空间进攻过程

##### 1) 隐藏己方位置

普通攻击者都会利用别人的计算机隐藏他们真实的 IP 地址。老练的攻击者还会利用 800 电话的无人转接服务连接因特网服务提供商 (ISP, Internet Service Provider), 然后再盗用他人的账号上网。

##### 2) 收集信息

尽可能多地收集目标的相关信息,为后续的“精确”攻击打下基础。这一阶段收集的信息包括网络信息(域名、IP 地址、网络拓扑)、系统信息(操作系统版本、开放的各种网络服务版本)、用户信息(用户标识、组标识、共享资源、即时通信软件账号、邮件账号)等。收集信息的主要方法:利用公开信息服务,主机扫描与端口扫描,操作系统探测与应用程序类型识别等。

##### 3) 漏洞挖掘

漏洞挖掘是指对未知漏洞的探索,综合应用各种技术和工具,尽可能地找出软件中的潜在漏洞。漏洞挖掘是一个多种漏洞挖掘分析技术相结合、共同使用和优势互补的过程。目前漏洞挖掘分析技术有多种,主要包括手工测试技术、Fuzzing 技术、比对和二进制比对技术、静态分析技术、动态分析技术等。

##### 4) 发起攻击

发起攻击可能有下列多种选择:

(1) 试图毁掉攻击入侵的痕迹，并在受到损害的系统上建立另外的新的安全漏洞或后门，以便在先前的攻击点被发现之后，继续访问这个系统。

(2) 在系统中安装探测软件，包括木马等，用以掌握一切活动信息，收集较感兴趣的信息。

(3) 如果在一个局域网中，攻击者就可能会利用被攻击的电脑作为对整个网络展开攻击的大本营，这时被攻击者不仅是受害者，而且还会成为帮凶和替罪羊。

#### 5) 获取权限

获取权限主要是获取目标系统的读、写、执行等权限。得到超级用户权限是攻击者在单个系统中的终极目标，因为得到超级用户权限就意味着对目标系统的完全控制，包括对所有资源的使用以及所有文件的读、写、执行等权限。获取权限的主要方法有：综合使用信息收集阶段收集到的所有信息，利用口令猜测、系统漏洞或者特洛伊木马对目标实施攻击。

#### 6) 设置后门

一般攻击者都会在攻入系统后反复地进入该系统，为了下次能够方便地进入系统，攻击者往往会留下一个后门。利用各种后门程序以及特洛伊木马，在目标系统中安装后门程序，以更加方便、更加隐蔽的方式对目标系统进行操控。

#### 7) 清除痕迹

消除攻击的痕迹，以尽可能长久地对目标进行控制，并防止被识别、追踪。这一阶段是攻击者打扫战场的阶段，其目的是消除一切攻击的痕迹，尽量做到被攻击者无法察觉系统已被侵入，否则至少也要做到使管理员无法找到攻击的发源地。清除痕迹的主要方法是针对目标所采取的安全措施清除各种日志及审核信息。

## 2. 黑客进攻流程

黑客要实施攻击，一般来说必须有 3 个基本步骤：

- (1) 收集信息（踩点）；
- (2) 选择目标，实施攻击；
- (3) 上传黑客程序，取得控制权，下载用户数据。

黑客入侵的一般模式为：踩点→查点→扫描→分析并入侵→获取权限→提升权限→扩大范围→安装后门→清除日志。黑客攻击行为流程的一般模型如图 6-3 所示。

图 6-3 中虚线框以上部分完成收集信息；虚线框中是入侵模块，即实施攻击；最后完成黑客攻击的目的。

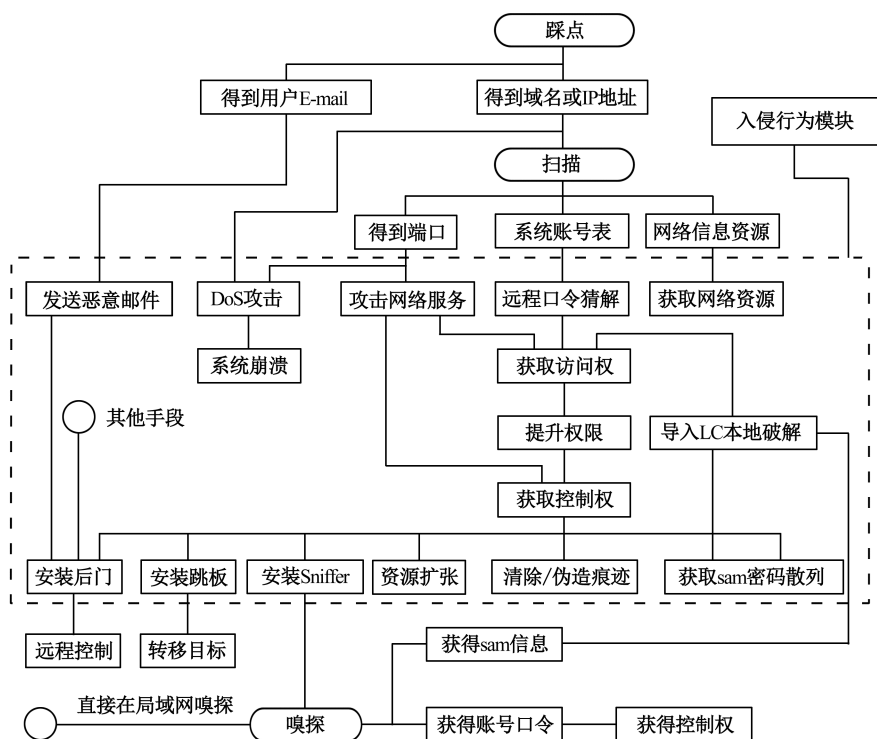


图 6-3 黑客攻击行为流程的一般模型

黑客攻击在第一步就是踩点，即收集信息，这也是黑客攻击的关键一步。收集汇总各种与目标系统相关的信息，包括目标网络结构、用户数、目标机器类型、用户 E-mail、所用域、IP 地址、操作系统、开放的端口、开放的应用服务、应用漏洞、保护性较差的数据传输、设备的品牌和型号等。另外，还要通过扫描获取端口号、系统账号表和网络信息资源。踩点是耗费时间最长的阶段，黑客会利用各种渠道尽可能多地了解被攻击对象的类型和工作模式，包括互联网搜索、社会工程、垃圾数据搜寻、域名管理/搜索服务、非侵入性的网络扫描等。

在第二步，选择用户 E-mail 发送恶意邮件，并安装后门；在获得域名、IP 地址用户端口号以后，展开 DoS 攻击，致使系统崩溃；得知端口号以后攻击网络服务；得知系统账号表以后对远程口令进行猜测；在提升和获取控制器以后，对资源进行扩张，清除/伪造痕迹，并为今后可能的访问留下控制权限。为了保证攻击的顺利完成，攻击者必须保持连接的时间足够长。虽然攻击者到达这一阶段也就意味着已成功地规避了系统的安全控制措施，但这也也会导致攻击者面临的漏洞增加。因此，关注反恶意软件、个人防火墙和基于主机的入侵检测解决方案，在任何不寻常活动出现的时间发出警告。

在第三步，通过安装后门和其他手段，实现远程控制；通过安装跳板转移目标；直接在局域网中展开嗅探和通过安装 Sniffer 进行嗅探，以便获得账号口令，并最终获得控制权，下载用户数据。

## 6.1.5 网络空间进攻性作战机理

网络空间进攻性作战机理是指在网络空间进攻性作战过程中的运行原理和制胜途径，是对网络空间作战规律与作战指导规律的深层次揭示。网络空间进攻进程如图 6-4 所示，从一个侧面反映了对网络空间进攻性作战机理的理解与认识。

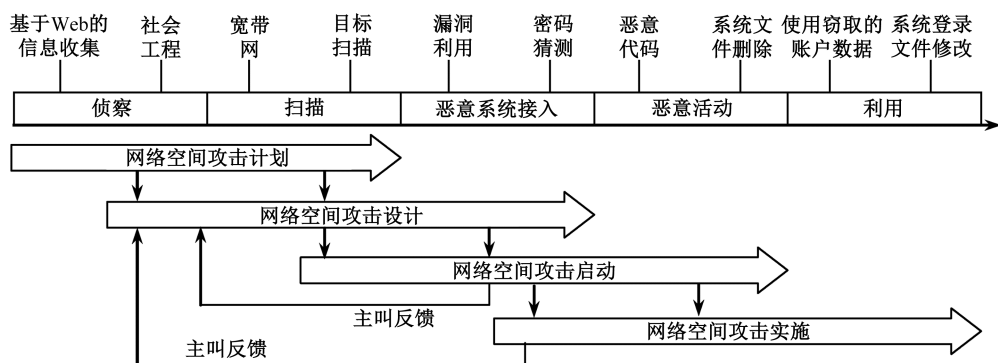


图 6-4 网络空间进攻进程

网络空间进攻性作战机理的核心内容是态势感知、控流入网、综合施效、破网毁体。具体地说，就是根据联合作战和网络空间作战需要，综合利用以技术为主的态势感知手段，获取网络空间相关部署、活动与信息；控制电磁能量流、电子信号流、数据信息流，有序进入敌方网络空间；高效发挥电磁信号层能量压制、数据信息层漏洞利用、心理认知层情绪诱导、物理设施层实体毁伤的综合破坏杀伤效应，通过断链、破网、毁体三个递进升级过程，破坏敌方网络空间的运行秩序与信息安全，瘫痪其作战体系和战争支撑体系。

### 1. 态势感知机理

主要是综合采取技术侦察、人力侦察、社会工程学等手段，重点查明敌、我、友、他等各方特别是敌方军事网、国家政务网、关键基础设施信息网和互联网等信息网络的情况。

(1) 物理设施层态势感知。主要对构成网络空间的物质基础——物理设施层进行侦察感知，即侦察信息网络的类型、物理空间位置、重要节点、网络拓扑结构、技术参数、安全漏洞和防护薄弱环节、军事价值等，为实施网络进攻、电子进攻和精确火力打击等提供目标情报保障和打击效果评估。

(2) 电磁信号层态势感知。主要对连接网络空间的传输媒介——电磁信号层进行侦察感知，即侦察信息网络的信息传输通道类型、物理空间位置、通信枢纽、技术参数、业务流量、安全漏洞与防护薄弱环节等，进一步分析与确定信息网络的网络拓扑结构、军事价值，为实施网络进攻、电子进攻和精确火力打击等提供目标情报保障和打击效果评估。

(3) 数据信息层态势感知。主要对构成网络空间的本质要素——数据信息层进行侦察感知，即侦察信息网络的有关数据信息。一是获取信息网络的操作系统软件、应用系统软

件、通信协议、安全管理系统软件等数据信息，为实施病毒攻击、拒绝服务攻击、数字大炮攻击等提供目标情报保障和打击效果评估。二是获取信息网络中产生、传输、存储、运行的数据信息。如敌方、相关国家（地区）或国家集团的政治、经济、军事、外交、科技、文化等情况，特别是敌方领导人、军方高级将领活动以及强敌出兵干预等核心内幕情况，为党中央、中央军委战略决策提供情报支援；及时掌握敌兵力部署调整、战争动员等情况，查明敌方重要目标、重兵集团和信息化主战武器装备动向、行动企图、战场环境等情况，综合分析战场态势、并预测其可能的发展趋势，为联合作战指挥员判断情况、定下决心、控制协调部队行动提供情报支援；侦察获取作战对象的网络空间作战计划、进攻防御能力以及作战动向，及早发现、跟踪、识别和报知来袭情况，向作战部队提供必要的信息支援。

（4）心理认知层态势感知。主要对网络空间的作用对象——心理认知层进行侦察感知，即侦察信息网络中的政治、军事、外交战略动向、公众关注热点等情况，进一步分析与确定心理进攻的特定人群、心理支点与弱点、信息传输途径与手段等。

## 2. 控流入网机理

与传统陆、海、空、天物理空间不同，在网络空间中流动的主要是电磁能量流、电子信号流、数据信息流。实施网络空间进攻，主要根据不同的作战目的、运用不同的手段、采取不同的方法，控制“三流”进入敌方网络空间。

（1）控制电磁能量流入网。核心是敌对双方争夺电磁频谱使用权和主导权的斗争，是利用电磁能、定向能来确定、扰乱、削弱、破坏、摧毁敌方电子信息系统和电子设备，进攻方式主要有电子干扰、电子欺骗、反辐射攻击、定向能摧毁。其进攻对象包括侦察预警、指挥控制、导航定位、武器制导、敌我识别等作战过程中的雷达、通信、光电、水声等依赖电磁频谱的各类设备和设施，也包括那些可能受到定向能影响的电子信息设备和设施。

（2）控制电子信号流入网。实质是对敌方电子信号的获取和利用，进攻方式主要有：主动注入具有欺骗性和破坏性的电子信号，进行信息仿冒和跳板渗透，进而获取敌网络控制权限，实施病毒破坏、网络控制和信息窃密等进攻行动。对电子信号的控制主要围绕密码展开，加密和破译成为攻防双方的斗争焦点。

（3）控制数据信息流入网。目的是利用网络进攻手段窃取敌方情报信息、控制或瘫痪敌方信息系统或基础设施。进攻方式主要有：一是系统入侵。利用系统的硬件、软件等各方面的漏洞，掌握系统访问权限和控制权，获取敌方的保密文件，删除、修改敌方系统中的数据或埋藏后门程序等。二是病毒攻击。把具有不同破坏功能的各种计算机病毒，通过无线注入、固化植入、黑客侵入、磁盘“摆渡”等方式，进入敌方军事或民用信息网络，以扰乱、瘫痪敌方信息网络和信息系统。三是 DDoS 攻击，集中互联网上的众多傀儡机，同时向一个目标或多个目标发送大量攻击性数据包，造成敌方网络和信息系统“淤积阻塞”，暂时无法使用。

下面介绍数字大炮攻击的机理。

数字大炮攻击是一种新型的 DDoS 攻击，其攻击过程和机理是：利用 BGP 自身特性，通过对路由器数据层面发起大规模攻击，使网络中路由器间互连链路反复拥塞，影响路由

器控制层面的信息交互，使数据层面无法转发数据，导致网络瘫痪。数字大炮攻击的机理模型如图 6-5 所示。

### 3. 综合施效机理

网络空间进攻是一种多层次的新型作战形式，凡电磁波和信息流所达之处皆可能成为战场。总体上讲，网络空间进攻就是综合运用电磁信号层的能量压制、数据信息层的漏洞利用、心理认知层的情绪诱导、物理设施层的实体毁伤这四种软硬结合的杀伤效应，如图 6-6 所示，达成对网络空间的控制权。

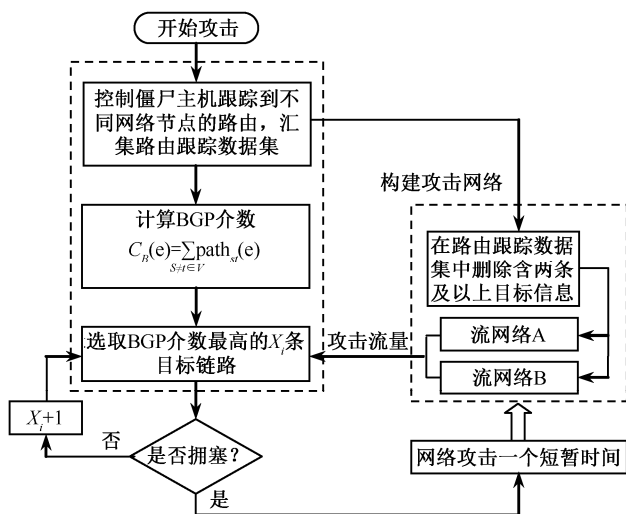
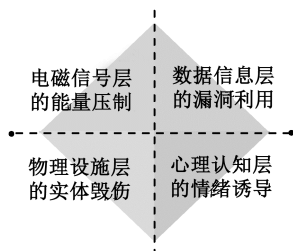


图 6-5 数字大炮攻击的机理模型

图 6-6 网络空间进攻的四种杀伤效应



(1) 能量压制，主要对敌通信、指控、雷达、导航、制导等系统的电磁信号，有意识地发射或转发频率对准、功率超过和样式耦合的电磁波，或实施全频段、高功率的阻塞式压制，使其不能正常工作。

(2) 漏洞利用，主要发掘信息网络和信息系统存在的固有缺陷，以此为突破口实施进攻破坏。漏洞种类包括：硬件漏洞，主要有电磁泄漏、预置芯片、设计缺陷等；软件漏洞，主要在程序编写、软件安装和运行环境设置中产生的错误和缺陷，以及人为设置的后门和陷阱；管理漏洞，包括权限管理、保密管理及身份确认中的策略失误和薄弱环节。漏洞发掘、利用和弥补的技术水平，是网络空间进攻作战的核心能力。

(3) 情绪诱导，主要通过信息媒介进攻敌方军民心理支点和弱点，导致其认知偏差、情感失控和意志崩溃，达成攻心夺志、不战而屈人之兵的目的。

(4) 实体毁伤，主要采用高能微波、电磁脉冲等新概念武器和反辐射打击手段，摧毁敌信息网络物理设施；利用传播特制病毒、恶意代码等方式，渗透到与网络连接的工业系统、基础设施和武器平台等实体的控制系统，进而对物理设备进行破坏。



#### 4. 破网毁体机理

破网毁体主要是通过断链、破网、毁体三个不断升级的过程,破坏敌方网络空间的运行秩序与信息安全,进而瘫痪其作战体系和战争支撑体系。其实质是各种网络作战效应作用于网络空间后向外扩散的过程,也是网络空间作战制胜机理作用于联合作战的过程。就当前而言,网络空间攻击应以“破网瘫网”为目标,核心是降低敌方信息网络的效能。远期,可以“控网”为目标,夺取敌方信息网络的控制权,让敌方信息网络为我所用。

(1) 断链。断敌信息链路既是网络空间作战的重要方式,也是破击体系的有效途径,其核心是破坏敌关键信息流程,使敌感知失聪、指挥失灵、时空失准、武器失控、保障失供,形不成体系作战能力。断侦察感知链,就是干扰破坏敌侦察监视和预警探测等战场感知系统,乱敌情报信息流程,切断情报获取、传输、处理、分发与共享的信息链路,使敌从源头上看不见、看不清、看不远。断指挥决策链,就是干扰破坏敌指挥信息系统,乱敌指令信息流程,切断决策、计划、组织、协调的信息链路,使敌在指挥上判不明、决不准、联不通。断武器控制链,就是干扰破坏嵌入武器平台和弹药的信息系统,乱敌武器控制信息流程,切断“从传感器到射手”的信息链路,使敌武器系统效能降低甚至失控。断导航定位链,就是干扰破坏敌卫星定位和导航系统,乱敌时空基准,切断获取空间位置和时间频率的信息链路,使敌在战场时空上丧失精确性和一致性。断综合保障链,就是干扰破坏敌后勤、装备等保障信息系统,乱敌保障信息流程,切断敌供、储、运、修的信息链路,使敌消耗补给难以及时准确到位。

(2) 破网。网络空间作战很大程度上就是破击、控制敌方军事信息网和战争潜力信息网,这也是瘫痪敌作战体系和战争体系的重要途径。破军事信息网,重点是对敌信息网络关键节点实施瘫毁进攻。比如,通过进攻敌侦察预警系统的雷达管报站、指控系统的通信枢纽站、数据链系统的组网中心等,可破坏敌作战体系整体结构,达成“毁一点、瘫一片”的效果。破战争潜力信息网,重点是对敌公共信息网、基础设施与关键业务信息网、工业控制网等实施进攻渗透。通过进攻敌电信网、国际互联网、广播电视网,以及银行、证券、电力、铁道、民航等信息网络,可有效扰乱经济秩序、破坏社会稳定、瓦解民心士气,从根本上动摇其战争意志,削弱其战争能力。

(3) 毁体。就是针对敌方作战体系和战争支撑体系严重依赖网络空间的弱点,打击其网络化信息系统,破坏其网络空间的运行秩序与信息安全,进而瘫痪敌方作战体系和战争支撑体系。主要表现在通过“断链”“破网”,盲敌预警、断敌通联、乱敌指控、扰敌精打、降敌综保,使敌看不清、联不通、控不住、打不准、保不上,导致敌方作战体系和战争支撑体系的效能下降直至崩溃。

态势感知、控流入网、综合施效、破网毁体是前后衔接、相互影响、共同作用的,是网络空间进攻作战的主要过程与方式。态势感知是网络空间进攻的逻辑起点,只有知道敌方网络空间地理位置在哪儿、物理构成如何、系统脆弱点是什么等,才能有效组织对敌方网络空间的进攻行动;控流入网是网络空间进攻的关键所在,只有控制电磁能量流、电子信号流、数据信息流进入敌方网络空间,网络空间进攻才有实施的可能,若无法进入敌方

网络空间，网络空间进攻就无从谈起；综合施效是网络空间进攻的作用方式，施效的成功与否主要取决于能否在敌方发现我网络空间进攻迹象、采取有效防御措施之前，最大限度地发挥各种网络空间进攻手段的破坏作用；破网毁体是网络空间进攻的追求结果，只有达到预期的断链、破网、控网目的，才算实现了网络空间进攻的作战目标。

## 6.2 网络空间进攻的主要手段

技术决定战术，掌握网络空间进攻的主要手段，是在作战中灵活运用战法，达到瘫痪网络空间系统目的的基础。当前，许多网络系统并不完善，系统配置存在着缺陷，由于网络用户和管理人员的疏忽造成系统诸多安全漏洞，这使得网络进攻人员有许多进攻取胜的机会。网络进攻的手段多种多样，已经发现的网络空间攻击手段达数千种之多。下面介绍几种主要的网络进攻手段，包括计算机病毒攻击、欺骗类攻击、拒绝服务攻击、口令攻击、缓冲区溢出攻击、Web 攻击、密码分析攻击。

### 6.2.1 计算机病毒攻击

计算机病毒是指具有破坏计算机功能或破坏数据，影响计算机使用并能够自我复制的一组计算机指令或程序代码，它具有以下特征：程序性、隐蔽性、寄生性、传染性、触发性、潜伏性、主动性、针对性、破坏性和不可预见性。计算机病毒的种类很多，包括复合型病毒、系统引导病毒、宏病毒、文件型病毒等。病毒破坏目标和攻击部位主要有系统数据区、文件、内存、系统运行、运行速度、磁盘、屏幕显示、键盘、喇叭、打印机、主板等。

#### 1. 病毒的工作流程

病毒一般都是通过各种方式把自己植入内存，获取系统最高控制权，以感染在内存中运行的程序。计算机病毒的完整工作过程应包括以下几个环节。

- (1) 传染源。病毒总是依附于某些存储介质，如 U 盘、硬盘等构成传染源。
- (2) 传染媒介。病毒传染的媒介由其工作的环境决定，可能是计算机网络，也可能是可移动的存储介质，如 U 盘等。
- (3) 病毒激活。它指将病毒装入内存，并设置触发条件。一旦触发条件成熟，病毒就开始自我复制到传染对象中，进行各种破坏活动等。
- (4) 病毒触发。计算机病毒一旦被激活，就会立刻发生作用。触发的条件是多样化的，可以是内部时钟、系统的日期、用户标识符，也可能是系统一次通信等。

(5) 病毒表现。表现是病毒的主要目的之一,有时在屏幕显示出来,有时则表现为破坏系统数据。凡是软件技术能够触发到的地方,都在其表现范围内。

(6) 传染。病毒的传染是病毒性能的一个重要标志。在传染环节中,病毒复制一个自身的副本到传染对象中去。计算机病毒的传染是以计算机系统的运行及读写磁盘为基础的。没有这样的条件,计算机病毒是不会传染的。只要计算机运行,就会有磁盘读写动作,病毒传染的两个先决条件就很容易得到满足。系统运行为病毒驻留内存创造了条件,病毒传染的第一步是驻留内存;一旦进入内存之后,寻找传染机会,寻找可攻击的对象,判断条件是否满足,决定是否可传染;当条件满足时进行传染,将病毒写入磁盘系统。

## 2. 病毒传染的方法

根据病毒传染的方法可分为驻留型病毒和非驻留型病毒。驻留型病毒感染计算机后,把自身的内存驻留部分放在内存中,这一部分程序挂接系统调用并合并到操作系统中去,它处于激活状态,一直到关机或重新启动。非驻留型病毒在得到机会激活时并不感染计算机内存,一些病毒在内存中留有小部分,但并不通过这一部分进行传染,这类病毒也被划分为非驻留型病毒。

## 3. 病毒注入的方法

实施病毒入侵的核心技术是解决病毒的有效注入。病毒注入的方法主要有以下方式。

(1) 无线电方式。主要通过无线电把病毒码发射到敌方网络系统中。这是计算机病毒注入的最佳方式,同时技术难度也最大。可能的途径有:①直接向敌方网络系统的无线电接收器或设备发射,使接收器对其进行处理并把病毒传染到目标机上。②冒充合法无线传输数据。根据得到的或使用标准的无线电传输协议和数据格式,发射病毒码,使之能够混在合法传输信号中,进入接收器,进而进入信息网络。③寻找敌方信息系统保护最差的地方进行病毒注放。通过对方未保护的数据链路,将病毒传染到被保护的链路或目标中。

(2) 后门攻击方式。后门是一个模块的秘密入口,即系统的后门。在程序开发期间,后门的存在是为了便于测试、更改和增强模块的功能。一般情况下,程序员不会把后门记入软件的说明文档,用户通常无法了解后门的存在。因此,后门形成了计算机安全系统中的一个漏洞,允许知道其存在的人绕过正常安全防护措施进入系统。攻击后门的形式有许多种,如控制电磁脉冲可将病毒注入目标系统。计算机入侵者就常通过后门进行攻击。

(3) “固化”方法。即把病毒事先存放在硬件(如芯片)和软件中,然后把此硬件和软件直接或间接交付给对方,使病毒直接传染给敌方网络系统,在需要时将其激活,达到攻击目的。这种攻击方法十分隐蔽,即使芯片或组件被彻底检查,也很难保证其没有其他特殊功能。目前,我国很多计算机组件依赖进口,因此,很容易受到芯片的攻击。

(4) 直接方式。直接派遣间谍或买通敌方人员,直接把病毒传染给敌方计算机,继而扩散到整个网络系统。

(5) 游戏方式。军队正在越来越多地使用个人计算机,不少工作人员将计算机游戏安装到了计算机的硬盘上,在指挥控制系统或其他密级很高的计算机系统上玩游戏。这样带

病毒的游戏软件便可以使病毒轻而易举地进入计算机。

(6) 数据控制链侵入方式。随着互联网技术在军事上的广泛应用,使计算机病毒经过网络空间的数据控制链侵入成为可能。运用远程修正技术,能很随便地改动数据控制链的正常路径。

(7) 捆绑式注入。使用特定的捆绑程序将病毒与一些应用程序如 QQ、IE 捆绑起来,表面上看是正常文件,当用户运行这些捆绑病毒时,会表面上运行这些应用程序,然后隐藏运行捆绑在一起的病毒,从而给敌方网络系统造成危害。如用 WinRAR 制作自解压文件,把想捆绑的程序一起压缩,在自解压选项里有一项“解压后运行”,再填上捆绑的程序的文件名,就可以使目标系统中毒。

(8) 远程控制木马注入。木马程序是比较流行的病毒文件,与一般的病毒不同,它不会自我繁殖,也不会感染其他文件。通过放置特洛伊木马程序使其直接侵入用户的计算机并进行破坏,它常被伪装成工具程序或游戏等诱使用户打开带有特洛伊木马程序的邮件附件或从网上直接下载。一旦被攻击者打开了这些邮件的附件或执行了这些程序之后,它们就会像古特洛伊人在敌人城外留下的藏满士兵的木马一样留在被攻击的计算机中,并在被攻击的计算机系统中隐藏一个可以在 Windows 启动时悄悄执行的程序。当被攻击者连接到互联网上时,这个程序就会通知攻击者,来报告被攻击的 IP 地址以及预先设定的端口。攻击者在收到这些信息后,再利用这个潜伏在其中的程序,就可以任意地修改被攻击的计算机的参数设定、复制文件、窥视被攻击的整个硬盘中的内容等,从而达到远程控制被攻击计算机的目的。

除上述病毒注入方式外,还有一些其他的方式,这里就不再详细介绍了。

#### 4. 病毒攻击原理

计算机病毒都是利用人性弱点或程序弱点攻入计算机系统的,其主要方式是通过直接或间接地攻击、破坏应用程序文件或系统程序文件来达到感染、传播和藏匿目的。

##### 1) 利用人性弱点的攻击原理

所谓利用人性弱点的攻击原理就是指病毒利用人与生俱来的好奇、贪婪等心理,采用带有社会工程学性质的欺骗手法来骗取用户信任,以达到攻入用户计算机系统的目的。如 CIH 病毒,利用人爱美、好奇等心理,将自己伪装成热门女主角“小龙女”的屏幕保护程序,诱惑大量用户下载并使用该屏保程序,致使该病毒达到广泛传播,给当时的计算机界带来了一次巨大的浩劫。又如,“库尔尼科娃”病毒的大流行便是利用了当时俄罗斯“网坛美女”库尔尼科娃难以抵挡的魅力。诸如此类的病毒还有“爱虫”(Love Letters)、“大无极”(Sobig.f)、“MyDoom”“维罗纳”等病毒,都是通过将病毒自身写入电子邮件的正文或伪装成附件,并为邮件的主题和附件起一个极具诱惑性或极易使人信任的名字,诱使用户打开带有病毒的邮件或附件,从而攻入计算机系统。如今,网络上充斥了大量伪装的带毒网页、电子邮件、各类图片、影音文件、常用的应用程序等,它们几乎都是企图利用人性弱点,诱使用户点击或下载。

近年来，新一代的病毒更加善于伪装和隐藏自己，它们在利用人性弱点的同时，更是将社会工程学原理运用得淋漓尽致，甚至利用了人们的各类社交活动、社会关系等来骗取对方信任，以得到运行自己的机会，最终达到传播自己、感染用户计算机系统的目的。

2) 利用程序弱点的攻击原理

利用程序弱点的攻击原理是指病毒利用操作系统程序或各类应用程序及其插件所存在的缺陷、漏洞等来攻击用户计算机系统，最终达到侵入系统的目的。如冲击波（Blaster）病毒，它利用了微软操作系统 Windows 2000/XP 的分布式组件对象模型（DCOM）RPC 缓冲区漏洞，在攻入用户计算机系统并取得完整的用户权限后，即可在受感染的计算机上执行任意的程序代码。此外，它还能利用所感染的计算机通过网络继续搜索，攻击网络上存在此漏洞的其他计算机。致使大量的计算机被感染。表 6-1 是部分典型病毒所利用的程序弱点及其攻击的主要方式。

表 6-1 部分典型病毒所利用的程序弱点及其攻击的主要方式

序号	病毒名称	所利用的程序弱点	攻击主要方式
1	Melissa	利用 Word 应用程序的宏脚本漏洞	攻击和破坏 Word 的模板文件
2	I LOVE YOU	利用 Outlook 应用软件漏洞	攻击和破坏*.mp3、*.vbs、*.jpg、*.hta、*.js 等文件
3	Code Red	利用 IIS 系统漏洞（idq.dll 远程缓冲器溢出）进行传播	攻击和破坏相应的进程
4	SQL Slammer	利用 SQL Server 2000 的解析漏洞进行缓冲区溢出攻击	攻击和破坏相应的进程
5	Bagle	利用 ActiveX 缺陷进行攻击	终止保护染毒计算机的应用程序进程
6	Sasser	利用 LSASS 的缓冲器溢出漏洞进行攻击	直接攻击、破坏 PE 文件
7	HappyTime	利用 Outlook Express 的安全漏洞进行攻击	攻击和破坏*.htm、*.html、*.vbs、*.asp 等文件
8	Nimda	利用 IE、因特网信息服务器（IIS，Internet Information Server）软件漏洞进行传播	攻击和破坏*.htm、*.html、*.exe、*.asp 等文件
9	求职信	利用 IE 漏洞进行攻击	终止某些反病毒软件进程
10	熊猫烧香	利用微软的 MS06-014 漏洞以及 QQ、UC 浏览器的漏洞	直接攻击*.html、*.exe、*.asp 等文件，并终止大量的反病毒软件进程

5. 10 种典型的病毒攻击

1) ARP 病毒攻击

ARP 病毒并不是某一种病毒的名称，而是对利用 ARP 的漏洞进行传播的一类病毒的总称。ARP 病毒攻击，是针对以太网 ARP 的一种攻击技术，就是通过伪造 IP 地址和 MAC 地址实现 ARP 欺骗。此种攻击能够在网络中产生大量的 ARP 通信量使网络阻塞，可让攻击者取得局域网上的数据封包甚至可篡改封包，且可让网络上特定计算机或所有计算机无法正常连接。攻击者只要持续不断地发出伪造的 ARP 响应包就能更改目标主机 ARP 缓存中的 IP-MAC 条目，造成网络中断或中间人攻击。

## 2) 蠕虫病毒攻击

蠕虫病毒是一种常见的计算机病毒，其前缀是 **Worm**。它是利用网络进行复制和传播的，传染途径包括文件、电子邮件、Web 服务器、网络共享等。最初的蠕虫病毒定义是因为在 DOS 环境下，病毒发作时会在屏幕上出现一条类似虫子的东西，胡乱吞吃屏幕上的字母并将其改形。蠕虫病毒是自包含的程序（或是一套程序），它能传播自身功能的拷贝或自身（蠕虫病毒）的某些部分到其他的计算机系统中（通常是经过网络连接）。

这种方式是利用操作系统和应用程序的漏洞主动进行攻击的。蠕虫病毒主要是“红色代码”（Code Red）和“熊猫烧香”，以及依然肆虐的“求职信”等。由于 IE 浏览器的漏洞，使得感染了“熊猫烧香”病毒的邮件在非手工打开附件情况下就能激活病毒。曾经流行的“熊猫烧香”以及其变种就是蠕虫病毒。这一病毒利用了微软视窗操作系统的漏洞，计算机感染这一病毒后，会不断自动拨号上网，并利用文件中的地址信息或网络共享进行传播，最终破坏用户的大部分重要数据。

## 3) 宏病毒攻击

宏病毒是一种寄存在文档或模板的宏中的计算机病毒。宏病毒的前缀是 **Macro**，第二前缀是 Word、Word97、Excel、Excel97（也许还有别的）其中之一。一旦打开这样的文档，其中的宏就会被执行，于是宏病毒就会被激活，转移到计算机上，并驻留在 Normal 模板上进行攻击。从此以后，所有自动保存的文档都会“感染”上这种宏病毒，如果其他用户打开了感染病毒的文档，宏病毒又会转移到他的计算机上。该类病毒的共有特性是能感染 Office 系列文档，然后通过 Office 通用模板进行传播，如著名的美丽莎（Macro.Melissa）。

## 4) 系统病毒攻击

系统病毒的前缀为 Win32、PE、Win95、W32、W95 等。这些病毒的一般共有的特性是可以感染和攻击 Windows 操作系统的\*.exe 和\*.dll 文件，并通过这些文件进行传播。如 CIH 病毒。

## 5) 引导型病毒攻击

引导型病毒是一种在只读内存（ROM, Read-Only Memory）基本输入输出系统（BIOS, Basic Input Output System）之后的引导区病毒。它先于操作系统，依托的环境是 BIOS 中断服务程序。引导型病毒是利用操作系统的引导模块放在某个固定的位置，并且控制权的转交方式是以物理位置为依据，而不是以操作系统引导区的内容为依据，因而病毒占据该物理位置即可获得控制权，而将真正的引导区内容搬家转移或替换，待病毒程序执行后，将控制权交给真正的引导区内存，使得这个带病毒的系统看似正常运转，而病毒已隐藏在系统中并伺机传染、发作并进行攻击。

## 6) 文件型病毒攻击

所有通过操作系统的文件系统进行感染的病毒都称作文件型病毒，所以这是一类数目

非常巨大的病毒。文件型病毒主要感染计算机中所有标准的磁盘操作系统（DOS，Disk Operating System）可执行文件（.exe）、命令文件（.com）、批处理文件和可加载驱动程序文件（.sys），以及感染所有视窗操作系统后缀名是 EXE、DLL 或者 VXD、SYS 的文件。这种病毒是对计算机的源文件进行修改，使其成为新的带毒文件。一旦计算机运行该文件就会被感染，从而达到传播和攻击的目的。

#### 7) 脚本病毒攻击

脚本病毒的前缀是 Script，如红色代码（Script.Redlof），通常是 JavaScript 代码编写的恶意代码，通过网页进行传播的病毒，一般带有广告性质，会修改对方的 IE 首页、修改注册表等信息，造成对方使用计算机不方便。脚本病毒还会有如下前缀：VBS、JS（表明用何种脚本编写），如欢乐时光（VBS.Happytime）、十四日（Js.Fortnight.c.s）等。

由于脚本是直接解释执行，并且它不需要像可移植的执行体（PE，Portable Executable）病毒那样，需要做复杂的 PE 文件格式处理，因此这类病毒可以直接通过自我复制的方式感染其他同类文件，并且自我的异常处理变得非常容易。其破坏力不仅表现在对用户系统文件及性能的破坏，还可以使邮件服务器崩溃，网络发生严重阻塞。

#### 8) 病毒种植程序病毒攻击

这类病毒的共有特性是运行时会从体内释放出一个或几个新的病毒到系统目录下，由释放出来的新病毒产生破坏和攻击。如冰河播种者（Dropper.BingHe2.2C）、MSN 射手（Dropper.Worm.Smibag）等。

#### 9) 破坏性程序病毒攻击

破坏性程序病毒的前缀是 Harm。这类病毒的共有特性是利用本身具有的好看图标来诱惑用户点击，当用户点击这类病毒时，病毒便会直接对用户计算机产生破坏和攻击。如格式化 C 盘（Harm.formatC.f）、杀手命令（Harm.Command.Killer）等。

#### 10) 玩笑病毒攻击

玩笑病毒的前缀是 Joke，也称恶作剧病毒。这类病毒的共有特性是利用本身具有的好看图标来诱惑用户点击，当用户点击这类病毒时，病毒会做出各种破坏操作来吓唬用户展开攻击，其实病毒并没有对用户计算机进行任何破坏。如女鬼（Joke.Girl ghost）病毒。

## 6.2.2 欺骗类攻击

下面介绍 6 类欺骗类攻击，即 ARP 欺骗攻击、DNS 欺骗攻击、IP 欺骗攻击、路由欺骗攻击、万维网（WWW）欺骗攻击和电子邮件欺骗攻击。

## 1. ARP 欺骗攻击

由于局域网的网络流通不是根据 IP 地址进行的，而是根据 MAC 地址进行传输，所以 MAC 地址在 A 上被伪造成一个不存在的 MAC 地址，这样就会导致网络不通，A 不能 Ping 通 C！这就是一个简单的 ARP 欺骗。而 ARP 欺骗攻击就是利用该协议漏洞，通过伪造 IP 地址和 MAC 地址实现 ARP 欺骗的攻击技术。

ARP 欺骗分为两种：一种是对路由器 ARP 表的欺骗；另一种是对内网个人计算机(PC, Personal Computer)的网关欺骗。第一种 ARP 欺骗的原理是截获网关数据。它通知路由器一系列错误的内网 MAC 地址，并按照一定的频率不断进行，使真实的地址信息无法通过更新保存在路由器中，结果路由器的所有数据只能发送给错误的 MAC 地址，造成正常 PC 无法收到信息。第二种 ARP 欺骗的原理是伪造网关。它的原理是建立假网关，让被它欺骗的 PC 向假网关发数据，而不是通过正常的路由器途径上网。在 PC 看来，就是上不了网了，“网络掉线了”。

一般来说，ARP 欺骗攻击的后果非常严重，大多数情况下会造成大面积掉线。有些网管员对此不甚了解，出现故障时，认为 PC 没有问题，交换机没掉线的“本事”，电信也不承认宽带故障。在第一种 ARP 欺骗发生时，只要重启路由器，网络就能全面恢复，那问题一定是在路由器了。为此，宽带路由器背了不少“黑锅”。

## 2. DNS 欺骗攻击

DNS 欺骗就是攻击者冒充域名服务器的一种欺骗行为。其原理：如果可以冒充域名服务器，然后把查询的 IP 地址设为攻击者的 IP 地址，那么用户上网就只能看到攻击者的主页，而不是用户想要取得的网站的主页了，这就是 DNS 欺骗的基本原理。DNS 欺骗其实并不是真的“黑掉”了对方的网站，而是冒名顶替、招摇撞骗罢了。

首先欺骗者向目标机器发送构造好的 ARP 应答数据包，ARP 欺骗成功后，嗅探到对方发出的 DNS 请求数据包，分析数据包取得标识符 (ID, Identifier) 和端口号后，向目标发送自己构造好的一个 DNS 返回包，对方收到 DNS 应答包后，发现 ID 和端口号全部正确，即把返回数据包中的域名和对应的 IP 地址保存进 DNS 缓存表中，而当真实的 DNS 应答包返回时则被丢弃，那么该 DNS 目标机器就被欺骗了。

假设嗅探到目标靶机发出的 DNS 请求包有以下内容：

Source address: 192.168.1.57

Destination address: ns.baidu.com

Source port: 1234

Destination port: 53 (DNS port)

Data: www.baidu.com

伪造的 DNS 应答包如下：

Source address: ns.baidu.com

Destination address: 192.168.1.57



Source port: 53 (DNS port)

Destination port: 1234

Data: www.baidu.com 192.168.1.59

目标靶机收到应答包后把域名及对应IP保存在了DNS缓存表中,这样www.baidu.com的地址就被指向到了192.168.1.59上。

网络进攻者通常通过以下几种方法进行DNS欺骗。

#### 1) 缓存感染

攻击者会熟练地使用DNS请求,将数据放入一个没有设防的DNS服务器的缓存当中。这些缓存信息会在客户进行DNS访问时返回给客户,从而将客户引导到入侵者所设置的运行木马的Web服务器或邮件服务器上,然后攻击者从这些服务器上获取用户信息。

#### 2) DNS信息劫持

攻击者通过监听客户端和DNS服务器的对话,通过猜测服务器响应给客户端的DNS查询ID。每个DNS报文有一个相关联的16位ID号,DNS服务器根据此ID号获取请求源位置。攻击者在DNS服务器之前将虚假的响应交给客户,从而欺骗客户端去访问恶意的网站。

#### 3) DNS重定向

攻击者能够将DNS名称查询重定向到恶意DNS服务器,这样攻击者可以获得DNS服务器的写权限。

### 3. IP欺骗攻击

IP欺骗是在服务器不存在任何漏洞的情况下,通过利用TCP/IP协议本身存在的一些缺陷进行攻击的方法,这种方法具有一定的难度,需要掌握有关协议的工作原理和具体的实现方法。

#### 1) IP欺骗攻击的原理

IP欺骗,简单来说就是向目标主机发送源地址为非本机IP地址的数据包。IP欺骗在各种黑客攻击方法中都得到了广泛的应用,比如,进行拒绝服务攻击,伪造TCP连接,会话劫持,隐藏攻击主机地址等。

IP欺骗的表现形式主要有两种:一种是攻击者伪造的IP地址不可达或根本不存在,如图6-7所示。这种形式的IP欺骗,主要用于迷惑目标主机上的入侵检测系统,或者是对目标主机进行DoS攻击。

另一种IP欺骗则着眼于目标主机和其他主机之间的信任关系。攻击者通过在自己发出的IP包中填入被目标主机所信任的主机的IP来进行冒充,如图6-8所示。一旦攻击者和目标主机之间建立了一条TCP连接(在目标主机看来,是它和它所信任的主机之间的连接。事实上,它是把目标主机和被信任主机之间的双向TCP连接分解成了两个单向的

TCP 连接), 攻击者就可以获得对目标主机的访问权, 并可以进一步进行攻击。

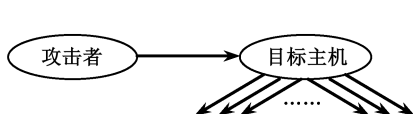


图 6-7 伪造无实际意义的 IP



图 6-8 攻击者伪装成被目标主机所信任的主机

## 2) IP 欺骗的攻击步骤

IP 欺骗的攻击步骤:

- (1) 首先使被信任主机的网络暂时瘫痪, 以免对攻击造成干扰;
- (2) 然后连接到目标机的某个端口来猜测初始序列号 (ISN, Initial Sequence Number) 基值和增加规律;
- (3) 接下来把源地址伪装成被信任主机, 发送带有 SYN 标志的数据段请求连接;
- (4) 然后等待目标机发送 SYN+ACK 包给已经瘫痪的主机;
- (5) 最后再次伪装成被信任主机向目标机发送的 ACK (Acknowledgement), 此时发送的数据段带有预测的目标机的 ISN+1;
- (6) 连接建立, 发送命令请求。

## 4. 路由欺骗攻击

在 TCP/IP 网络中, IP 数据包的传输路径完全由路由表决定。若攻击者通过各种手段改变路由表, 使目标主机发送的 IP 包到达攻击者能控制的主机或路由器, 就可以完成嗅探监听和篡改等攻击方式。路由欺骗通常有以下几种方式。

### 1) RIP 路由欺骗

RIP 协议用于自治系统内传播路由信息。路由器在收到 RIP 数据报时一般不做检查。攻击者可以声称他所控制的路由器 A 可以最快地到达某一站点 B, 从而诱使发往 B 的数据包由 A 中转。由于 A 受攻击者控制, 攻击者就可以侦听、篡改数据了。

### 2) IP 源路由欺骗

IP 报文首部的可选项中有“源站选路”, 可以指定到达目的站点的路由。正常情况下, 目的主机如果有应答或其他信息返回源站, 就可以直接将该路由反向运用作为应答的回复路径。

主机 A (假设 IP 地址是 192.168.100.11) 是主机 B (假设 IP 地址为 192.168.100.1) 的被信任主机, 主机 X 想冒充主机 A 从主机 B 获得某些服务。首先, 攻击者修改距离 X 最近的路由器 G2, 使用到达此路由器且包含目的地址 192.168.100.1 的数据包以主机 X 所在的网络为目的; 然后, 攻击者 X 利用 IP 欺骗 (把数据包的源地址改为 192.168.100.11) 向主机 B 发送带有源路由选项 (指定最近的 G2) 的数据包。当 B 回送数据包时, 按收到数据包的源路由选项反转使用源路由, 传送到被更改过的路由器 G2。由于 G2 路由表已被

修改, 收到 B 的数据包时, G2 根据路由表把数据包发送到 X 所在的网络, X 可在其局域网内较方便地进行侦听, 收取此数据包。

### 3) 基于 ICMP 的路由欺骗

ICMP 的重定向报文是由路由器发送给报文信源机的, 告诉它应该将报文发送到另一个路由器。当一个主机接收到 ICMP 重定向报文时, 它就会修改自己的路由表, 通过发送非法的 ICMP 重定向报文来进行路由欺骗。为防止这类路由欺骗, 一个主机可配置为忽略 ICMP 重定向报文, 也可在收到 ICMP 重定向报文时检查该报文是否确实来自刚才使用过的路由器。

### 4) 基于 RIP 的路由欺骗

RIP 是使用非常普通的距离决定路由算法。它通常使用报文中转次数、时间延迟、等待队列长度等作为距离来决定路由。使用协议的机器可分为两类: 主动的和被动的。运行 RIP 协议的路由器是主动的, 它每隔 30 秒广播一报文, 其中包含其他机器的 IP 地址及到该地址的距离。与路由器相邻的机器收到报文就修改它的路由表。被动的机器是不广播的, 仅接收并修改路由表。只有路由器可以处于主动模式, 主机只能处于被动模式。一个简单的路由欺骗是, 通过 UDP 在端口 520 (RIP 的端口) 广播非法的路由信息, 所有参与 RIP 协议的被动的机器都会受到影响, 尤其有路由器处于被动状态时, 这种损害就会传播开来。防范这种欺骗的措施是禁止或限制路由器处于 RIP 协议的被动状态。

## 5. 万维网 (WWW) 欺骗攻击

用户在网上可以利用 IE 等浏览器进行各种各样的 Web 站点的访问, 如阅读新闻组、咨询产品价格、订阅报纸、电子商务等。然而一般的用户恐怕不会想到有这些问题存在: 正在访问的网页已经被黑客篡改过, 网页上的信息是虚假的! 例如, 黑客将用户要浏览的网页的用户路由表 (URL, User Route List) 改写为指向黑客自己的服务器, 当用户浏览目标网页的时候, 实际上是向黑客服务器发出请求, 那么黑客就可以达到欺骗的目的了。

## 6. 电子邮件欺骗攻击

电子邮件欺骗 (E-mail spoofing) 是伪造电子邮件头, 导致信息看起来来源于某个人或某个地方, 而实际却不是真实的源地址。垃圾邮件的发布者通常使用欺骗和恳求的方法尝试让收件人打开邮件, 并很有可能让其回复。电子邮件假冒和欺骗形式多样, 有的在电子邮件中声明该邮件是来自系统管理员, 要求用户修改口令 (口令可能为指定字串), 并威胁如果不服从则采取某种措施; 有的电子邮件声称来自某一授权人, 要求用户发送其口令文件或其他敏感信息的拷贝。

目前使用的简单邮件传送协议 (SMTP, Simple Mail Transfer Protocol) 极其缺乏验证功能, 假冒电子邮件进行电子邮件欺骗是不难的。可以使用假冒的发信人邮件地址, 而邮件服务器并不对发信人身份的合法性做任何检查。如果站点允许和 SMTP 端口连接, 任何

人都可以连接到该端口（25），并发一些假冒用户或虚构用户的邮件。这时候，在邮件中就会很难找出与发信人有关的真实信息，唯一可以追查的只能是检查系统的日志文件，找出这封邮件是从哪台主机发出的；然后，再检查发信的那台主机，看看那段时间，有什么用户在使用，但很难找出伪造者。用户也可能修改其 Web 浏览器用来发送假冒的电子邮件，也可以使用 Telnet 直接登录到接收邮件服务器的 TCP 端口 25 来发送假冒的电子邮件。

在邮件欺骗中，收信人的用户名是真的，发送用的邮件服务器也是真的；然而，发信人的邮件地址是假的。从邮件中，根本无法知道是谁发出了这样一封邮件，邮件的内容也就无法保证了。当邮件服务器是一台公共使用的主机时，或者用户在发送完毕之后清除自己的上机记录，另外更换主机名和 IP 地址也是非常容易的。在这种情况下，伪造的邮件就会很难追查下去了。

### 6.2.3 拒绝服务攻击

拒绝服务（DoS）攻击是网络进攻者较常使用的一种攻击手段。所谓的 DoS 攻击，是攻击者利用合理的密集式的服务请求来占用过多的服务资源，致使系统超载和服务器资源耗尽，无法响应其他的请求，从而达到对其攻击的目的。这些服务资源包括网络带宽、文件系统空间容量、开放的进程或向内的连接。

其具体表现方式有以下几种：

（1）制造大流量无用数据，造成通往被攻击主机的网络拥塞，使被攻击主机无法正常和外界通信。

（2）利用被攻击主机提供服务或传输协议上处理重复连接的缺陷，反复高频地发出攻击性的重复服务请求，从而使该服务分配的资源耗尽，使被攻击主机停止提供服务（包括中断服务器进程、重新配置系统、填充进程表和整个文件系统、进程崩溃），无法及时处理其他正常的请求。

（3）利用被攻击主机所提供服务程序或传输协议的本身实现缺陷，反复发送畸形的攻击数据引发系统错误地分配大量系统资源，使处理程序进入死循环，使主机处于挂起状态甚至死机。

#### 1. DoS 的攻击过程

首先攻击者向被攻击者发出带有虚假用户地址的合理请求，被攻击者回复请求后等待用户响应消息，由于用户地址是虚假的，被攻击者无法得到相应的用户响应，在等待一段时间后该连接和相应的资源才会因超时而释放。在此期间连接会占用一定的服务器和网络资源，当服务器接收到过多的这种连接时就会耗尽资源，而对正常用户的服务请求产生拒绝现象，由此产生拒绝服务攻击。DoS 的攻击过程如图 6-9 所示。

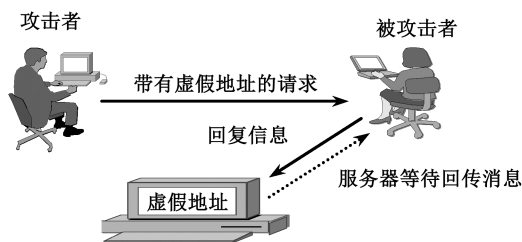


图 6-9 DoS 的攻击过程

2. DoS 的攻击手段和方法

DoS 的攻击手段和方法有以下几种。

1) 资源消耗型攻击

网络需要一定的资源才能运行，如网络带宽、存储器、磁盘空间、CPU 时间和数据结构等。攻击者利用系统资源有限这一特点，可以发起拒绝服务攻击，消耗系统匮乏的、有限的或不可再生的资源。资源消耗型攻击的过程示意图如图 6-10 所示。

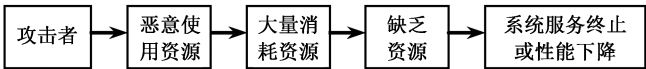


图 6-10 资源消耗型攻击的过程示意图

根据攻击过程中使用的系统资源，资源消耗型攻击可以进一步分为消耗网络带宽、消耗磁盘空间、消耗 CPU 资源和内存资源。

(1) 消耗网络带宽攻击。攻击者有意制造大量的广播包或传输大量文件以消耗有限的网络可用带宽，致使合法的用户无法正常使用网络资源，从而实现攻击者的意图。攻击者可以采用系统工具软件 Ping、Finger 来制造大量的广播包或数据包。在 Ping-Flooding 拒绝攻击中，攻击者通过连续使用 Ping 命令向网络中的某个目标主机或服务器发出大量的 ICMP-ECHO-REQUEST 数据包，使目标主机也必须发出对应的 ICMP-ECHO-REPLY 包来响应。这样造成的后果可能有几种：一是这些大量的 ICMP-ECHO-REQUEST 包和 ICMP-ECHO-REPLY 包也同时出现在网络中，将会使网络速度降低，而合法用户的网络传输速度将显著降低，在极为严重的情况下甚至连接也将会中断；二是目标主机不得不忙于处理这些 ICMP-ECHO-REQUEST 请求响应数据包，而合法的用户将不能与该主机建立连接，也就无法获得正常的服务；三是会导致被攻击的目标系统崩溃、重新启动或挂起。许多系统和路由器对这种拒绝服务攻击都非常敏感。因此，Ping-Flooding 也是一种较为典型的拒绝服务攻击。

还有一种更有效的消耗网络带宽的攻击方法叫作 Smurf 攻击。在 Smurf 攻击中，它并不直接对目标主机发送服务请求包。所谓的 Smurf 攻击是指攻击者找出网络上有哪些路由器会回应 ICMP 请求，并在远程机器上发送 ICMP 应答请求服务，其目标主机不是某一个主机的 IP 地址，而是某个网络的广播地址，其请求包的源 IP 不是发起攻击的 IP 地址，而

是加以伪装的将要攻击的主机 IP 地址，大量主机收到 ICMP 应答请求服务包后，按照源 IP 返回请求信息，同时产生大量信息流，从而占用所有设备的资源及网络带宽，导致受攻击主机的服务性能下降，甚至崩溃。由于 Smurf 攻击中运用了多点多路同步攻击的先进手段，可以更有效地使目标系统的网络端口阻塞，拒绝为正常系统进行服务，同时也更好地隐藏了攻击者，保护攻击者不易被受攻击者发现。

(2) 消耗磁盘空间攻击。攻击者消耗受害节点磁盘空间的方法有很多，但归纳起来主要有以下几种。

①发送大量的 E-mail 信息。电子邮件缺少对源发送方的检查及邮件系统提供的 E-mail-List 功能，攻击者利用邮件系统这个功能制造大量的垃圾邮件。

②故意制造出错 Log 信息。某些系统提供出错信息记录功能，攻击者就故意制造出错 Log 信息，如 UNIX 系统的 Syslog 功能和 WWW 服务器的 Error-Log 功能。

③故意制造垃圾邮件。攻击者以合法的身份进入系统，然后编制 Shell 程序，故意制造垃圾文件。如在 UNIX 系统中，/temp 目录对普通用户都是可写的，攻击者可以编制一个小 Shell 程序不断地在该目录下制造一些垃圾文件，从而将系统可分配的磁盘空间消耗干净。

④在匿名 FTP 站点的公开目录下或网络邻居的共享区域下放置大量的垃圾邮件。

总之，任何允许向磁盘上写信息的机制，如果没有对所写数据的数量限制，都可被用来实施 DoS 攻击。

(3) 消耗 CPU 资源和内存资源攻击。一些系统提供的 CPU 资源和内存资源是由许多程序公用的，攻击者利用系统的特点，任意使用大量的 CPU 资源和内存资源，从而导致服务性能下降甚至造成系统崩溃。经常发生的服务端口攻击也属于这类拒绝服务攻击。服务端口攻击又称为服务请求过载攻击，每种网络服务都有其唯一的端口号。服务端口攻击就是攻击在网络服务器（主机）某些端口上运行的网络服务，使其减低或失去服务能力，严重时使系统崩溃或网络瘫痪。其基本方法是，在网络环境下，攻击者故意地、不断地向目标网络服务器（主机）发送大量的服务请求，当大量的服务请求发向目标主机的服务守护程序时，使得目标主机十分忙碌地处理这些不断带来的服务请求，以至无法处理常规的任务。同时，许多新到来的服务请求会被丢弃，因为没有内存空间来存放这些服务请求。这样就会发生服务过载，使其不能提供正常的网络服务，严重时会使系统崩溃或网络瘫痪，从而阻止合法的用户使用网络服务。

TCP SYN-Flooding 就是这样一种攻击方式，攻击者与受害节点建立连接，但是不最终完成。由于受害节点需要保持数据结构用于等待完成这些半连接，结果导致合法的连接因为缺乏数据结构资源而无法正常工作。在这种攻击中，攻击者消耗的是核心数据结构，而不是网络带宽。这意味着攻击者可以通过一个慢的网络，如拨号网络来攻击一个高速网络上的机器，这是一种典型的“非对称攻击”。

信息轰炸也属于资源消耗型攻击。信息轰炸就是攻击者向目标网络上的一台主机发送大量的数据包，来延缓目标主机的处理速度，阻止它处理正常的任务。这些请求可能是请求文件服务、要求登录或简单的请求响应包（如 Ping）。无论采用什么形式，这些潮水般

的服务请求，加重了目标主机的处理器负载，使目标主机消耗了大量的资源来响应这些请求。在极端情况下，这种攻击可以引起目标主机因为没有内存来缓存到来的请求，或者因为程序处理错误而死机。这类拒绝服务攻击是一种主动的信息轰炸攻击法，轰炸使用的信息称为信息炸弹。

电子邮件轰炸同样属于这一类拒绝服务攻击。对付消耗资源型攻击的方法是建立资源分配模型图，统计敏感的计算资源使用情况，使用限额方法及早检测并发现计算资源出现异常的情况。

2) 配置修改型攻击

计算机配置不当可能造成系统运行不正常甚至根本不能运行。攻击者通过改变或破坏系统的配置信息来阻止其他合法用户使用计算机和网络提供的服务，可使用的方法主要有以下几种：改变路由信息；修改 Windows NT 注册表；修改 UNIX 系统的各种配置文件，如 /etc 目录下的各种文件。这种模式的攻击示意图如图 6-11 所示。

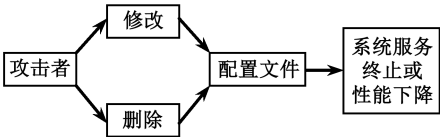


图 6-11 配置修改型攻击示意图

3) 物理破坏型攻击

这种拒绝服务攻击针对的是物理设备的安全。攻击者可以通过物理上破坏或改变网络中的组件以实现拒绝服务攻击。其攻击的目标有计算机、路由器、网络配线室、网络干线、电源、冷却设备等。

4) 服务请求过载攻击

服务请求过载攻击是指不断地向目标主机的 TCP/IP 服务端口发出连接请求，造成该端口来不及响应新的连接请求，从而不能提供正常的网络服务而崩溃，它相当于不停地打某人的电话，使某线路始终处于忙状态，以至正常的电话也打不进去。在 TCP/IP 网络中，



图 6-12 TCP 连接的三次握手过程

所有服务都是通过服务端口提供的，并且服务器上各服务端口的编号是固定的，同时 TCP 连接是通过“三次握手”的过程建立的，如图 6-12 所示。在正常情况下，请求连接的机器（客户机）发送一个信息包（SYN）请求建立连接，服务器以一个肯定应答（ACK）做出响应，客户机接着返回自己的肯定应答（ACK），一个连接就这样建立了。

当 ACK 包发送给客户机时，服务器一方要保留一部分内存，用以保存当前所建立的连接状态信息。除非收到客户机一方发回的 ACK 包或超时，否则这部分内存不会被其他任务使用，并且服务器将一直等待。由于 TCP 连接需要通过三次握手来建立一个连接与

设置参数，如果攻击者发出多个连接请求，初步建立了连接，但又没有完成其后的连接步骤，于是服务器便保留了许多这种半连接，占据着大量的资源。通常这些连接请求使用的都是伪造的源 IP 地址，连接来自一台不存在的主机或一台无法访问的主机，所以连接根本无法完成。服务器唯一可做的是等待，直到这个连接因为超时而释放。这类攻击典型的方法有 SYN-Flooding 攻击。

SYN-Flooding 攻击利用了 TCP 协议实现上的一个缺陷，通过向网络服务所在端口发送大量的伪造源地址的攻击数据包，造成目标服务器中的半开连接队列被占满，从而阻止其他合法用户进行访问。请求者（攻击者）的机器发出一系列连接请求，启动服务器端的三次握手过程，但是对服务器（被攻击者）的响应不做肯定应答。由于服务器始终接收不到肯定应答，它就一直等待。如果服务器不断地接收到这样的连接请求，端口将始终处于忙碌状态。在典型的 SYN-Flooding 攻击中，攻击者会使用一个伪装的地址向目标主机发送网络连接请求（叫作 SYN）。当目标主机收到这样的请求后，就会使用一些资源来为新的连接提供服务，接着回复请求一个肯定应答（叫作 SYN-ACK）。由于 SYN-ACK 是返回到一个伪装的 IP 地址，因此肯定不会有任何响应（叫作 ACK）。于是目标主机将继续设法发送 SYN-ACK。一些系统都有默认的回发次数和超时时间，只有回复一定的次数或超时，占用的资源才会释放。Windows NT 4.0 中默认设置为可重复发送 SYN-ACK 答复 5 次、每次重新发送后，等待时间翻番。第一次等待时间为 3 秒，到第 5 次重发 SYN-ACK 时，机器将等待 48 秒以求得响应。如果还是收不到响应，机器还要等待 96 秒，才取消分配给此连接的资源。在这些资源获得释放之前，已经过去了 189 秒。这样将一系列的 SYN 信息包发送给服务器，并且这些信息包使用伪造的源 IP 地址，当然服务器接收不到肯定应答。发送一段时间的 SYN 信息包后，攻击者就可用无法完成的请求阻塞服务器。攻击者尽可能地发送这样的请求，以便占用目标主机尽量多的资源，将目标主机“置于死地而后快”。

在这种情况下，服务器能做的事情极其有限。当然可以修改服务器操作系统的源码，使它有一个可调的超时值；加强日志记录功能；在拒绝新到来的连接之前，对同时存在的半连接数目有一个限制。然而，这些修改并不那么容易，防火墙也没有重视这个问题。最好的方法就是拒绝那些防火墙外面的未知主机或网络的连接请求。另一个办法是，对使用的协议增加一些限制。然而，任何固定的限制都是不适当的。

#### 5) 电子邮件轰炸

电子邮件炸弹也被称为 E-mail Bomber，指的是电子邮件的发送者利用某些特殊的电子邮件软件，在很短的时间内连续不断地将大容量的电子邮件邮寄给同一个收信人，而一般收信人的邮箱容量是有限的，攻击者能够耗尽接收者网络的宽带，在这些数以千计的大容量信件面前肯定是不堪重负的，而最终会“爆炸身亡”。

这种攻击手段不仅会干扰用户的电子邮件系统的正常使用，甚至它还能影响邮件系统所在的服务器系统的安全，造成整个网络系统全部瘫痪。因为它可以大量消耗网络资源，常常导致网络阻塞，使大量的用户不能正常工作。通常，互联网服务商给一般的网络用户



的信箱容量都是很有限的，如果用户在短时间内收到成千上万封电子邮件，而每个电子邮件的容量也比较大，那么经过一轮邮件炸弹轰炸后的电子邮件的总容量很容易就把用户有限的阵地挤垮。这些电子邮件炸弹所携带的大容量信息不断在网络上来回传输，很容易堵塞带宽并不富裕的传输信道，从而导致了整个过程的延迟。如果网络接入服务提供者承受不了这样的疲劳工作，网络随时也都会瘫痪，严重的可能会引发整个网络系统崩溃。因此也就成为一种拒绝服务攻击。

### 3. 分布式拒绝服务攻击

#### 1) 概念与模型

在 DoS 攻击的基础上，分布式拒绝服务（DDoS）攻击是指攻击者借助客户/服务器技术，将多台计算机（攻击者一般将这些被攻陷的多台计算机叫作傀儡机）联合起来作为攻击平台，对一个或多个目标发动 DoS 攻击，从而成倍地提高拒绝服务攻击的威力，这样就能极为暴力地将原本处理能力很强的目标服务器攻陷。由此可知，DDoS 与 DoS 的最大区别是数量。DoS 相对于 DDoS 来说就像是一个个体，而 DDoS 是大量的 DoS 的集合。另外，DDoS 攻击方式较为自动化，攻击者把他的攻击程序安装到网络中的多台傀儡机上，所采用的这种攻击方式很难被攻击对象察觉，直到攻击者发布统一的攻击命令，这些机器才同时发起进攻。图 6-13 为分布式拒绝服务攻击模型。

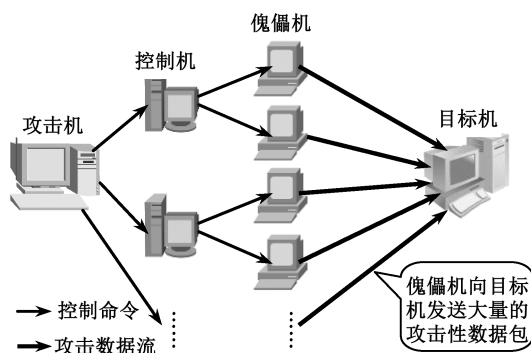


图 6-13 分布式拒绝服务攻击模型

DDoS 是一种基于 DoS 攻击，采用分布式、协作式的攻击方法。DDoS 攻击模型包括四个部分：攻击机、目标机、控制机和傀儡机。攻击机是指攻击者本人的主机，通过它下达分布式拒绝服务攻击的指令，组织和发起分布式拒绝服务攻击。控制机是指直接受攻击机控制的主机，但一般不属攻击者所有，数目通常为 3~4 台，并且在这些计算机上安装有特定的主控制软件。控制主机只发布命令而不参与实际的攻击。傀儡机是指被攻击者控制但一般并不为攻击者所拥有的计算机群。攻击者在这些计算机上安装了守护程序，运行并产生 DDoS 攻击代码，目标机是指攻击者要进行攻击的主机。攻击机向控制机，控制机向傀儡机发送控制命令；傀儡机向目标机发送大量的攻击性数据包。

## 2) DDoS 攻击的特征

遭到 DDoS 攻击后,常见的特征表现为:目标机上有大批等待的 TCP 连接;数据流中充满着大批的无用的数据包,源地址为假;服务器处理能力满负荷,或频繁死机或重新启动;链路中存在大量高流量无用数据,造成数据链路拥塞,使目标机无法正常和外界通信;利用目标机可以提供服务或传输协定这一缺点,重复高速地发出特定的服务请求,使目标机无法实时处置全部正常请求。

## 3) DDoS 攻击步骤

攻击机想要进行 DDoS 攻击,一般需要经历以下 3 个步骤:

(1) 获取目标信息。攻击者获取的目标信息主要有:目标机数目、配置、性能、地址情况;目标的带宽。

(2) 占领傀儡机。攻击者寻找在互联网上有漏洞的主机,最感兴趣的主机有三个基本条件:链路状态好、性能好、安全管理水平差。

傀儡机越多,攻击队伍就越壮大。攻击者占领傀儡机的方法有多种,如扫描端口、安置后门程序、网站恶意链接等。目前,获得大量傀儡机最有效的方法是通过携带后门程序的蠕虫,通过蠕虫的传播,后门程序就被安装到受蠕虫感染的傀儡机上。因此,这些傀儡机被攻击者侵占并安装上了攻击程序,随时等待攻击者的命令。

(3) 实际攻击。攻击者登录到作为控制台的傀儡机,并向所有的傀儡机发出攻击命令,这时候存于傀儡机中的 DDoS 攻击程序就会响应控制机的命令,一起向目标机以高速度发送大量的数据包,形成一股 DoS 洪流冲击目标系统,导致目标机死机或无法响应正常的请求,甚至系统瘫痪崩溃,达到攻击效果。

现在 DDoS 攻击的工具主要有 Trinoo、Tribe Flood Network (TFN)、TFN2K 和 Stacheldraht 等。

## 6.2.4 口令攻击

口令攻击是指攻击者以口令为攻击目标,破解合法用户的口令,或避开口令验证过程,然后冒充合法用户潜入目标网络系统,夺取目标系统控制权的过程。攻击者攻击目标时常常把破译用户的口令作为攻击的开始。口令是网络系统的第一道防线。当前的网络系统都是通过口令来验证用户身份、实施访问控制的。只要攻击者能猜测或确定用户的口令,他就能获得机器或网络的访问权和管理权,并能访问用户能访问的任何资源,窃取系统信息、磁盘中的文件,甚至对系统进行破坏。

### 1. 口令攻击的技术

口令攻击模型可用图 6-14 来表示。由此可见,有 3 种口令攻击方式,即从用户主机

中获取口令、在通信线路上截获口令、从远端系统中破解口令。

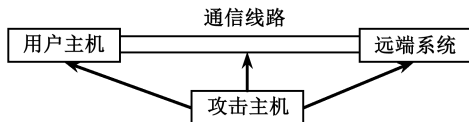


图 6-14 口令攻击模型

### 1) 从用户主机中获取口令

根据攻击者是否具有对用户主机的使用权可分为两种：一是具有使用主机的一般权限；二是不具有使用主机的任何权限。前者多见于一些特定场所，如企业内部、大学的计算中心、机房、网吧等。所破解的密码有 Word、Excel、Access 的办公文件，BIOS 密码，网吧管理软件的密码等。所使用的工具多为从网上下载的专用软件。这并不要求破解者有很高的技术水平，只要具备使用软件的一般能力就可进行破解。对于后者一般要有一定的技术水平。比如通过缓冲区溢出等攻击方法取得系统控制权后，通过安装木马或键盘记录器来窃取用户的各种口令。

键盘记录器是一种可以记录键盘操作的软件。在 Windows 系统中，在键盘上按下任何一个键都会产生按键消息，系统将该消息发送给相应的应用程序，交由应用程序去处理。使用钩子（Hook）技术和动态链接库（DLL，Dynamic Link Libraries）技术，攻击者可以截获这些按键消息，并对消息进行相应的处理，比如记录下所按的键并保存到文件中。

### 2) 在通信线路上截获口令

由于网络的特殊结构使得攻击者可以利用嗅探技术截取在通信线路上传输的口令信息。嗅探监听的原理图如图 6-15 所示。

嗅探器是一种利用网络接口截获目的地计算机数据报文的程序。在合理的网络中，嗅探器的存在对于系统管理员来说是很重要的，但若为某些人所使用却可以造成用户口令的泄露。

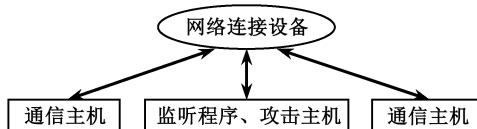


图 6-15 嗅探监听的原理图

嗅探器将本地计算机网卡的状态设置为混杂模式使它可以接收所遇到的每一个帧。若所接收到的帧中含有用户的口令信息，就可以通过程序显示出来。

### 3) 从远端系统中破解口令

这里的远端系统是指 Web 服务器或攻击者欲入侵的其他服务器。破解的口令有 E-mail、基于 Web 的访问口令、系统中一般用户和管理员的口令等。

攻击者入侵系统时，常常把破译系统中普通用户口令作为攻击的开始。因为只要取得系统中一般的访问权限，就很容易利用系统的本地漏洞来取得系统的控制权。

## 2. 口令攻击的方法

### 1) 穷举攻击法

穷举法对纯数字的密码有很好的破解效果，但若密码中含有一字线、半字线、浪纹线或其他字符就不适合采用这种方式。它的原理是逐一尝试数字的所有排列组合，直到破解出密码或尝试完所有组合为止。比如，对 6 位纯数字的密码，有 10 的 6 次方即 1 000 000 种可能，若每秒尝试 1 万次，则只需 100 秒的时间就可以遍历所有的可能性。

### 2) 字典攻击法

由于某些用户喜欢使用英文单词，将姓名拼音、生日、数字或这些字符的简单组合作为密码，因而攻击者就可以先建立包含大量此类单词的密码字典，然后使用程序一一尝试字典中的每个单词，直到破解出密码或字典被遍历为止。

### 3) 强行破解法

许多人认为如果使用足够长的口令，或者使用足够完善的加密模式，就能有一个攻不破的口令。事实上没有攻不破的口令，这只是个时间问题。如果有速度足够快的计算机能尝试字母、数字、特殊字符的所有组合，将最终破解所有的口令。这种类型的攻击方式叫强行攻击。使用强行攻击，先从字母 a 开始，尝试 aa、ab、ac 等，然后尝试 aaa、aab、aac 等。作为用户的口令尝试登录，如果口令错误，就按序取出下一个单词再进行尝试，直到找到正确的口令或字典的单词测试完为止。由于这个破译过程由计算机程序来自动完成，因而几个小时就可以把数十万条字典里的所有单词都尝试一遍。这种方法不受网段限制，但攻击者要有足够的耐心和时间。

### 4) 利用 Web 页面欺骗法

攻击者将用户所要浏览的网页 URL 地址改写成指向自己的服务器，当用户浏览目标网页的时候，实际上是一个伪造的页面，如果用户在这个伪造页面中填写有关的登录信息，如账户名称、密码等，这些信息就会被传送到攻击者的 Web 服务器，从而达到骗取的目的。如网上钓鱼就采取这种方式获取用户的银行卡号与密码等信息的。

### 5) 暴力破解法

想方设法获取服务器上的用户口令文件（此文件成为 Shadow 文件）后，用暴力破解程序破解用户口令。这种方法在所有方法中危害最大，因为它不需要像第三种方法那样一遍又一遍地尝试登录服务器，而是在本地将加密后的口令与 Shadow 文件中的口令相比较就能非常容易地破获用户密码，尤其那些对自己不负责任的用户（指口令安全系数极低的用户，如某用户账号为 zys，其口令就是 zys666、666666 或干脆就是 zys 等）更是在短短的一两分钟内，甚至几十秒内就可以将其破解。

## 6.2.5 缓冲区溢出攻击

### 1. 概念

缓冲区是计算机内存中存放数据的地方。从程序的角度来说,缓冲区就是应用程序用来保存用户输入数据、程序临时数据的内存空间。

进程使用的内存可以按照功能大致分成以下4个部分:(1)代码区,这个区域存储着被装入执行的二进制机器代码,处理器会到这个区域取出并执行;(2)数据区,用于存储全局变量等;(3)堆区,进程可以在堆区动态地请求一定大小的内存,并在用完之后归还给堆区。动态分配和回收是堆区的特点;(4)栈区,用于动态地存储函数之间的调用关系,以保证被调用函数在返回时恢复到调用函数中继续执行。

缓冲区溢出是一种非常普遍、非常危险的漏洞,在各种操作系统、应用软件中广泛存在。缓冲区溢出是指当计算机向缓冲区内某一个位置填充数据时,因为没有足够的空间而超过了缓冲区本身的容量,就会发生缓冲区溢出。溢出的数据覆盖在合法数据上,理想的情况是程序检查数据长度并不允许输入超过缓冲区长度的字符,但是绝大多数程序都会假设数据长度总是与所分配的储存空间相匹配,这就为缓冲区溢出埋下隐患,从而破坏程序的堆栈,使程序指针跳转而执行其他指令。操作系统所使用的缓冲区又被称为堆栈。在各个操作进程之间,指令会被临时储存在堆栈当中,堆栈也会出现缓冲区溢出。大多造成缓冲区溢出的原因是程序中没有仔细检查用户输入参数而造成的。

而人为的溢出则是有一定企图的。所谓缓冲区溢出攻击是利用缓冲区溢出漏洞所进行的攻击行动,是一种系统攻击手段。攻击者通过精心编写的带有某种攻击企图可执行代码(shellcode)的程序,通过在缓冲区写入超过预定长度的数据造成的溢出,破坏了堆栈的缓存数据,程序的返回地址发生变化,使它指向溢出程序中 shellcode 的开始,这样就可以运行攻击者的代码,使溢出送到能够以 root 权限运行命令的区域,以此获得超级控制权限、执行任意指令或达到其他攻击目的。

### 2. 危害

利用缓冲区溢出攻击,可以导致程序运行失败、系统崩溃、系统关机、重新启动等后果。更为严重的是,利用它可以执行非授权指令,甚至取得系统特权,进而进行各种非法操作。第一个缓冲区溢出攻击——Morris 蠕虫,曾造成了全世界 6000 多台网络服务器瘫痪。

缓冲区溢出中,最为危险的是堆栈溢出,因为入侵者可以利用堆栈溢出,在函数返回时改变返回程序的地址,让其跳转到任意地址,带来的危害当中,一种是程序崩溃导致拒绝服务,另一种就是跳转并且执行一段恶意代码,比如得到 shell,然后为所欲为。

### 3. 攻击的步骤

#### 1) 放入预先安排的代码

为使缓冲区溢出后截获程序的执行权限，攻击者需预先在系统中安置代码。一般情况下，攻击者需要一定的权限进行这类操作，代码也可以安置在数据段和堆栈段中，也可以使用已经存在的程序，这些程序主要包括一些系统调用程序，攻击者可以通过它们执行预先设置的程序。若不能放入或使用预先安置的代码，缓冲区溢出攻击类似于利用系统漏洞的拒绝服务攻击。

#### 2) 发现并利用缓冲区溢出

攻击者用其掌握的程序向有缓冲区溢出漏洞的程序输入一个超长的数据，造成缓冲区结构的破坏。这类超长的数据包含对返回地址的修改数据，因此，被攻击者程序将返回到攻击者希望的地址。如果缓冲区附近还存在函数指针或跳转地址，攻击者或其掌握的程序也可以利用修改它们的方法将程序指针 IP 指向其所希望的地址。

#### 3) 执行预先安排的代码

在 IP（指令指针）已经指向攻击者预先安排的代码时，这段代码开始执行，它一般具有和被攻击程序相同的权限，可以执行任何权限所允许的操作。

### 4. 攻击的原理

程序执行时的内存从逻辑上可以分为代码区和数据区两大部分，而数据区又可以分为静态数据区、堆栈和堆 3 个部分。代码区存放可执行代码，只能读不能写，因此相对较安全；数据区的数据经常随着程序的运行变化，是攻击发生的主要地方。

堆栈（简称栈）是一种先进后出的数据表结构。栈有两种常用操作：压栈和出栈。栈有两个重要属性：栈顶和栈底。内存的栈区实际上指的是系统栈。系统栈由系统自动维护，用于实现高级语言的函数调用。每一个函数在被调用时都有属于自己的栈帧空间。当函数被调用时，系统会为此函数开辟一个新的栈帧，并把它压入栈中，所以正在运行的函数总在系统栈的栈顶。当函数返回时，系统栈会弹出该函数所对应的栈帧空间。

Win32 系统提供了两个特殊的寄存器来标志系统栈顶端的栈帧。

扩展堆栈指针（ESP，Extend Stack Pointer）：该寄存器存放一个指针，它指向系统栈顶端那个函数栈的栈顶。

扩展基址指针（EBP，Extend Base Pointer）：该寄存器存放一个指针，它指向系统栈最顶端那个函数栈的栈底。

此外，扩展指令指针（EIP，Extend Instruction Pointer）寄存器对于堆栈的操作非常重要，EIP 包含将被执行的下一条指令的地址。

函数栈帧：ESP 和 EBP 之间的空间为当前栈帧，每一个函数都有属于自己 ESP 和 EBP。ESP 表示了当前栈帧的栈顶，EBP 标志了当前栈帧的栈底。

下面以在堆栈中的溢出说明缓冲区溢出攻击的原理。

堆栈是在程序运行过程中由操作系统分配的内存区域，当程序中发生函数调用时，主要完成如下操作：首先把函数参数压入堆栈；然后向堆栈压入指令寄存器（IR，Instruction Register）中的内容，作为返回地址（RET，RETurn address）；接下来放入堆栈的是基地址寄存器（EBP），把当前的栈指针（ESP）拷贝到 EBP，作为新的基地址；最后把 ESP 减去适当的数值，为本地变量留出一定空间。堆栈的结构如图 6-16 所示。

栈顶
缓冲区
基地址寄存器
返回地址
函数参数
栈底

图 6-16 堆栈的结构

通过以下程序执行过程可以说明对堆栈的操作和溢出的产生过程。

```
#include<stdio.h>
int main(){
char strbuffer[10];
gets(strbuffer);
printf("%s", strbuffer);}
```

编译运行以上代码，输入“network”结果会输出 network，其中对堆栈的操作是先在栈底压入返回地址，接着将栈指针 EBP 入栈，此时 EBP 等于现在的 ESP，之后 ESP 减 10，即向上增长 10 个字节，用来存放 strbuffer 数组。最后，从 main 返回，弹出 RET 里的返回地址并赋值给 IR，CPU 继续执行 IR 所指向的命令。如果输入的字符串长度超过 10 个字节，则由于输入的字符串太长，strbuffer 数组容纳不下，只好向堆栈的底部方向继续写入。这些超出 10 字节部分的数据覆盖了堆栈的基地址寄存器、RET 或函数参数部分的数据。从 main 返回时，就必然会把新的数据视作返回地址，CPU 会试图执行新数据所指向的指令，结果出现难以预料的后果，这样就产生了一次堆栈溢出。

除了上述攻击外，还有针对堆的溢出攻击和基于 lib 库的缓冲区溢出攻击及格式化串的攻击，无论是何种攻击，最根本的原因是 C 语言的 char\*这种数据结构的存在。在进行字符串处理时不能自动进行长度的检查，留下了很多的安全隐患。

5. 利用缓冲区溢出进行攻击的方式

缓冲区溢出攻击的目的在于扰乱具有某些特权运行的程序的功能，这样可以使得攻击者取得程序的控制权，如果该程序具有足够的权限，那么整个主机就被控制了。为了达到这个目的，攻击者必须达到以下两个目标：在程序的地址空间里安排适当的代码；通过适当的初始化寄存器和内存，让程序跳转到事先安排的地址空间执行。

1) 在程序的地址空间里安排适当的代码的方法

(1) 植入法。攻击者向被攻击的程序输入一个字符串，程序会把这个字符串放到缓冲区里。这个字符串包含的资料是可以在这个被攻击的硬件平台上运行的指令序列。在这里，攻击者用被攻击程序的缓冲区来存放攻击代码。缓冲区可以设在任何地方：堆栈（stack，

自动变量)、堆 (heap, 动态分配的内存区) 和静态资料区。

(2) 利用已经存在的代码。有时攻击者想要的代码已经在被攻击的程序中了, 攻击者所要做的只是对代码传递一些参数。例如, 攻击代码要求执行 `exec (“/bin/sh”)`, 而在 `libc` 库中的代码执行 `exec(arg)`, 其中 `arg` 是一个指向一个字符串的指针参数, 那么攻击者只要把传入的参数指针改为指向 `“/bin/sh”`。

## 2) 控制程序转移到攻击代码的方法

所有的这些方法都是在寻求改变程序的执行流程, 使之跳转到攻击代码。最基本的就是溢出一个没有边界检查或其他弱点的缓冲区, 这样就扰乱了程序的正常的执行顺序。通过溢出一个缓冲区, 攻击者可以用暴力的方法改写相邻的程序空间而直接跳过了系统的检查。原理上攻击时所针对的缓冲区溢出的程序空间可为任意内存地址, 但根据内存空间定位的不同, 主要有以下三种方式:

(1) 活动记录 (Activation Records)。每当一个函数调用发生时, 调用者会在堆栈中留下一个活动记录, 它包含了函数结束时返回的地址。攻击者通过溢出堆栈中的自动变量, 使返回地址指向攻击代码。当函数调用结束时, 程序就跳转到攻击者设定的地址, 而不是原先的地址。这是目前最常用的缓冲区溢出攻击方式。

(2) 覆盖函数指针 (Function Pointers)。函数指针可以用来定位任何地址空间。所以攻击者只需在任何空间内的函数指针附近找到一个能够溢出的缓冲区, 然后溢出这个缓冲区来改变函数指针。在某一时刻, 当程序通过函数指针调用函数时, 程序的流程就按攻击者的意图实现了。它的一个攻击范例就是在 Linux 系统下的 `superprobe` 程序。

(3) 长跳转缓冲区 (Longjmp buffers)。在 C 语言中包含了一个简单的检验/恢复系统, 称为 `setjmp/longjmp`。意思是在检验点设定 `“setjmp(buffer)”`, 用 `“longjmp(buffer)”` 来恢复检验点。然而, 如果攻击者能够进入缓冲区的空间, 那么 `“longjmp(buffer)”` 实际上是跳转到攻击者的代码。像函数指针一样, `longjmp` 缓冲区能够指向任何地方, 所以攻击者所要做的就是找到一个可供溢出的缓冲区。

## 3) 综合代码植入和流程控制

攻击者定位一个可供溢出的自动变量, 然后向程序传递一个很大的字符串, 在引发缓冲区溢出, 改变活动记录的同时植入了代码。代码植入和缓冲区溢出不一定要在一次动作内完成。攻击者可以在一个缓冲区内放置代码 (这个时候, 并不能溢出缓冲区), 然后, 攻击者通过溢出另外一个缓冲区来转移程序的指针。这种方法一般用来解决可供溢出的缓冲区不够大 (不能放下全部的代码) 的情况。如果攻击者试图使用已经常驻的代码而不是从外部植入代码, 通常必须把代码作为参数调用。举例来说, 在 `libc` (几乎所有的 C 程序都要它来连接) 中的部分代码段会执行 `“exec(something)”`, 其中 `something` 就是参数。攻击者使用缓冲区溢出改变程序的参数, 然后利用另一个缓冲区溢出使程序指针指向 `libc` 中的特定的代码段。



## 6.2.6 Web 攻击

Web 攻击的主要方式有 SQL 注入攻击、跨站脚本攻击和网页挂马等，下面分别加以介绍。

### 1. SQL 注入攻击

SQL 注入攻击是一种已经长期存在但近年来日益增长的安全威胁，是现在 Web 网站远程渗透最为有效的攻击方式，其注入技术的门槛低、攻击隐蔽、危害性大。一旦形成注入漏洞，网站 Web Shell 权限被攻击者获取，攻击者上传网页木马，从而控制整站，达到攻击目的。

#### 1) SQL 注入攻击的定义

SQL 注入攻击是利用 Web 应用程序的设计漏洞来实现 Web 应用系统，尤其是数据库的入侵，从而最终达到获取或破坏数据的一种策略及手段。攻击者有针对性地构造 SQL 语句，把 SQL 命令插入到 Web 表单的输入域或页面请求的查询字符串中，将其注入存在安全漏洞的网站后台数据库引擎中，并蓄意引导数据库服务器执行这些 SQL 语句，通过截取用户名和密码等重要信息，从而全面获取数据库控制权限。在某些表单中，用户输入的内容直接用来构造或影响动态 SQL 命令，或者作为存储过程的输入参数，这类表单特别容易受到 SQL 注入攻击。

SQL 注入攻击的主要形式有两种：一是直接将代码插入与 SQL 命令串联在一起并同时执行的用户输入变量中，由于其直接与 SQL 语句捆绑，所以也被称为直接注入攻击法；二是一种间接的攻击方法，它将恶意代码写入要在数据库表存储的字符串中，存储的字符串会连接到一个动态的 SQL 命令，以执行一些恶意的 SQL 代码。

#### 2) SQL 注入形成原因

SQL 注入攻击是由于程序员在编写代码过程中，对 SQL 语句书写不规范，对一些特殊字符没有过滤，导致在客户端能通过全局变量 POST 和 GET 提交一些 SQL 语句，远程获取服务器敏感信息，包括用户名、密码、姓名、电话、家庭住址等。

#### 3) SQL 注入攻击的危害

SQL 注入攻击的主要危害包括：非法读取、篡改、添加、删除数据库中的数据；获取数据库高级操作权限；盗取用户的各类敏感信息，获取利益；通过修改数据库来修改网页上的内容；私自添加或删除账号；注入木马；本地溢出并获得服务器最高权限；等等。

由于 SQL 注入攻击一般利用 SQL 语法，这使得基于所有 SQL 语言标准的数据库软件，如 SQL Server、Oracle、MySQL、DB2 等都有可能受到攻击，并且攻击的发生和 Web 编程语言本身也无关，如 ASP、JSP、PHP，在理论上都无法完全幸免。

SQL 注入攻击的危险是比较大的。很多其他的攻击，如 DoS 等，可能通过防火墙等

手段进行阻拦，但是对于 SQL 注入攻击，由于注入访问是通过正常用户端进行的，所以普通防火墙对此不会发出警示，一般只能通过程序来控制，而 SQL 攻击一般可以直接访问数据库，进而甚至能够获得数据库所在的服务器的访问权，因此，危害相当严重。

#### 4) SQL 注入攻击原理

SQL 命令是前端 Web 和后端数据库之间的接口，很多站点都利用 SQL 语句查询数据库，从而返回用户需要的信息。由于开发程序员编程水平参差不齐，在编程时没有对一些客户端编写的字符进行合法性检查过滤，导致攻击者在 URL 连接、表单域输入他们编写的 SQL 命令，查询出数据库的敏感信息，形成 SQL 注入攻击。

#### 5) SQL 注入攻击流程

SQL 注入攻击手段和方法多种多样，但总的来说，一般分为判断 Web 网站能否注入、寻找 SQL 注入点、猜解用户名和密码、上传网页木马、入侵和破坏五个阶段。

(1) 判断 Web 网站能否注入。如果网站全部做成静态化，访问网页时连接变成 `http://www.***.com/index.html`，这种普通网页访问，由于没有数据库访问入口，所以是不存在注入漏洞的。当访问网页变成 `http://www.***.com/do?id=1` 时，其中“`?id=1`”表示数据查询变量，这种语句需要在数据库端执行，因此通过单引号法判断程序是否存在注入漏洞。

(2) 寻找 SQL 注入点。寻找 SQL 注入点的经典查找方法是在有参数传入的地方添加“`and l=1`”“`and l=2`”，以及“`'`”等一些特殊字符，通过浏览器所返回的错误信息来判断是否存在 SQL 注入，若返回错误，则表明程序未对输入数据进行处理，绝大部分情况下都能进行注入。

(3) 猜解用户名和密码。数据库中现有的表名都是有规律的。攻击者可以通过构建特殊 SQL 语句在数据库中依次查找表名、字段名、用户名、密码长度和内容。这个猜测过程可以通过网上现有 SQL 注入工具快速实现，并借助破解网站轻易破译用户密码。

(4) 上传网页木马。在猜解到用户名和密码后，利用第三方扫描工具快速扫描网站，利用社会工程学反复尝试，从而获得网站管理员后台登录界面。登录到网站后台，利用上传功能上传网页木马。

(5) 入侵和破坏。在成功上传了网页木马后，接下来就可以进行任意的破坏行为，包括删除网站程序文件、篡改网页、添加非法用户、修改泄露用户信息，进一步入侵数据库从而获取数据库的控制权限。

## 2. 跨站脚本攻击

#### 1) 跨站脚本攻击的定义

跨站脚本 (XSS, Cross Site Scripting) 漏洞是 Web 应用程序在将数据输出到网页的时候存在问题，导致攻击者可以将构造的恶意数据显示在页面的漏洞。XSS 攻击是向 Web 页面内容中写入一段恶意的脚本或 html 代码，当用户浏览该页时，嵌入其中 Web 里面的 html 代码会被执行，从而达到恶意用户的特殊目的。与 SQL 注入攻击数据库服务器的方

式不同，跨站脚本漏洞是在客户端发动攻击，也就是说，利用跨站脚本漏洞注入的恶意代码是在用户计算机上的浏览器中运行的。

由于和另一种网页技术——层叠样式表（CSS，Cascading Style Sheets）的缩略语一样，为了防止混淆，故把原本的 CSS 称为 XSS。

## 2) 类型

XSS 攻击分成两类：一类是来自内部的攻击，主要指利用程序自身的漏洞，构造跨站语句；另一类则是来自外部的攻击，主要指攻击者构造 XSS 跨站漏洞网页或寻找非目标机以外的有跨站漏洞的网页。XSS 有三类跨站：①持久型跨站，最直接的伤害类型，跨站代码存储在服务器（数据库）中；②非持久型跨站，反射型跨站脚本漏洞，最普遍的类型，用户访问服务器—跨站链接—返回跨站代码；③文档对象模型（DOM，Document Object Model）跨站，客户端脚本处理逻辑导致的安全问题。

## 3) 跨站脚本攻击的原理

存储型跨站脚本攻击原理：将攻击代码提交到服务器端的数据库或文件系统中，不用构造 URL，而是保存在文章或论坛帖子中，从而使得访问该页面的用户都有可能受到攻击。

反射型跨站脚本攻击原理：在存在 XSS 漏洞网页的 URL 中插入脚本程序构造 URL，将 URL 通过邮件等发送给用户（钓鱼），当用户点击链接时，执行攻击者的脚本，一般是窃取用户的 Cookies 等个人数据、将用户导向恶意网站等。

## 4) 跨站脚本攻击的危害

该攻击的危害有：

- （1）网络钓鱼，盗取各类用户账号，如网银、管理员等账号；
- （2）欺骗浏览器访问钓鱼网站，窃取用户 Cookies 资料，从而获取用户隐私信息，骗取账号密码，进行非法转账等；
- （3）将使用者浏览器导向恶意网站，向使用者计算机下载并安装恶意后门程序，劫持用户（浏览器）会话，修改用户设置，做虚假广告，强制发表日志和发送电子邮件等；
- （4）进行恶意操作，如任意篡改页面信息、删除文章等；
- （5）网页挂马，进行大量的客户端攻击，如 DDoS 攻击；
- （6）获取客户端信息，如用户的浏览历史、真实 IP、开放端口等；
- （7）控制受害者机器向其他网站发起攻击；
- （8）结合其他漏洞，实施进一步作恶；
- （9）提升用户权限，包括进一步渗透网站；
- （10）传播跨站脚本蠕虫等。

## 3. 网页挂马攻击

### 1) 网页挂马攻击的定义

网页挂马攻击就是攻击者通过在正常的页面中插入一段恶意代码。若浏览者的浏览器

或浏览器加载的组件存在漏洞，那么他在打开该页面的时候，这段代码被执行，然后下载并运行某木马的服务器端程序。

## 2) 网页挂马攻击常见方式

(1) 将木马伪装为页面元素。木马则会被浏览器自动下载到本地。

(2) 利用脚本运行的漏洞下载木马并释放隐含在网页脚本中的木马。

(3) 将木马伪装为缺失的组件，或和缺失的组件捆绑在一起（如 Flash 播放插件）。这样既达到了下载的目的，下载的组件又会被浏览器自动执行。

(4) 通过脚本运行调用某些 com 组件，利用其漏洞下载木马。如 script 挂马是通过 script 的调用来挂马，可以直接挂 html 文件或挂 js 文件，可用明文挂马，也可加密挂马。

(5) 图片伪装挂马。将网页 x.htm 中的木马代码植入 x.gif 图片文件中。

(6) 在渲染页面内容的过程中利用格式溢出释放木马（如 ani 格式溢出漏洞），或者是下载木马（如 Flash9.0.115 的播放漏洞）。

## 3) 网页挂马攻击执行方式

(1) 利用页面元素渲染过程中的格式溢出执行 shellcode 进一步执行下载的木马。

(2) 利用脚本运行的漏洞执行木马。

(3) 伪装成缺失组件的安装包被浏览器自动执行。

(4) 通过脚本调用 com 组件利用其漏洞执行木马。

(5) 利用页面元素渲染过程中的格式溢出直接执行木马。

(6) 利用 com 组件与外部其他程序通信，通过其他程序启动木马（如 realplayer10.5 存在的播放列表溢出漏洞）。

## 4) 网页挂马的行为

在与网页挂马斗争的过程中，为了躲避杀毒软件的检测，一些网页挂马具有以下行为：

(1) 修改系统时间，使杀毒软件失效。

(2) 摘除杀毒软件的 Hook 挂钩，使杀毒软件检测失效。

(3) 修改杀毒软件病毒库，使之检测不到恶意代码。

(4) 通过溢出漏洞不直接执行恶意代码，而是执行一段调用脚本，以躲避杀毒软件对父进程的检测。

## 4. 其他方式 Web 攻击

### 1) 信息泄露

一般通过提交特殊的错误参数，Web 服务器返回特定的详细的敏感信息，漏洞成因一般有 Web 程序对错误处理不严、服务器配置不当、Web 开发和管理不当等。

2) 社会工程学

社会工程学攻击是指通过收集攻击目标相关信息甚至直接与攻击目标相接触等非技术的手段实施攻击的办法，在收集到攻击目标足够多的信息时，社会工程学的能量是十分强大和恐怖的，但却往往被人忽视。

3) 上传漏洞

上传漏洞是指利用上传功能，绕过上传文件安全控制，通常方法有三种：本地 Java 描述语言（JS，Java Script）安全控制检测文件格式类型；Content-type 判断绕过；空字节绕过。

6.2.7 密码分析攻击

因为密码学是创建密码的科学和艺术，密码分析（cryptanalysis）就是破解密码的科学和艺术。密码分析攻击有四类，如图 6-17 所示。

1. 纯密文攻击

在纯密文攻击中，张三只能访问一些密文。他要设法找到相关的密钥和明文。假设张三知道这种算法并可以破解这个密文，因为张三在这次攻击中需要的就是密文，纯密文攻击就是最可能被采用的方法。为了避免被对手解密，密码必须对这种攻击具有有效的抵抗。如图 6-18 所示的就是纯密文攻击的过程。

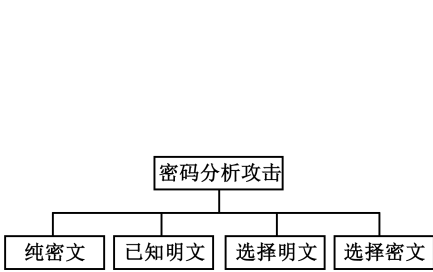


图 6-17 密码分析攻击

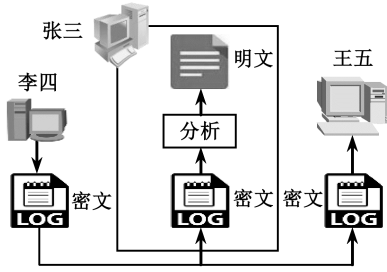


图 6-18 纯密文攻击的过程

多种方法可以被应用于纯密文攻击中，这里只提出几种普通的类型。

1) 蛮力攻击

在蛮力攻击（brute-force method）或穷举攻击中，张三试图使用所有可能的密钥。假设张三知道算法和密钥域（所有密钥的目录），运用拦截密码的方法，张三采用所有可能的密钥对密文进行解密，直到明文被搞清楚。在过去，用蛮力攻击是困难的，今天使用计

算机就容易多了。为了避免此类攻击，密钥的数量必须足够大。

## 2) 统计攻击

发动统计攻击所用的明文语言的内在特点，对密码分析是有益的。例如，知道字母 E 是英语文本当中最常用的字母，密码分析者就要找出密文当中使用最多的字母，并且假设相关明文的字母就是 E。找出几对之后，分析者就可以找到密钥并运用这把密钥去解密信息。为了避免这种攻击，密码应当把语言特征隐藏起来。

## 3) 模式攻击

有些密码可能会把语言特征隐藏起来，不过也可能在密文当中创建一些模式。密码分析者可能会用模式攻击来破解密码。所以，运用那些可以使密文尽可能混乱的密码就显得很重要。

# 2. 已知明文攻击

在已知明文攻击中，如图 6-19 所示，除拦截以后需要破解的密文以外，张三还访问了一些明文/密文对。

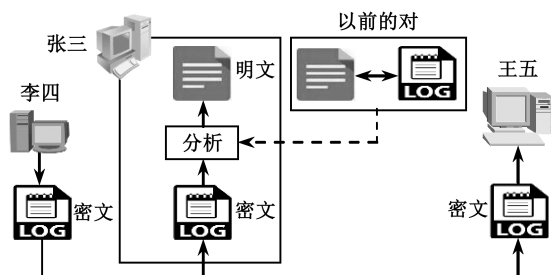


图 6-19 已知明文攻击

早先明文/密文对会被收集起来。例如，李四给王五发出一条密信，但是后来他又公开了这一密信的内容。张三把明文和密文都保存起来，如果李四还用原来的密钥，张三就可以破解李四和王五之间的下一个密信了。张三运用以前的明文和密文对就可以分析现在的密文。用在纯密文攻击当中的相同的方法，在这里也可以被利用。因为张三拥有较多的可以用来分析的信息，实现这种攻击还是比较容易的。然而，如果李四不公开以前信息的内容或改变密钥，这种攻击就无从实现了。

## 3. 选择明文攻击

选择明文攻击和已知明文攻击相似，不过明文/密文对是由攻击者自己选择的。如图 6-20 所示的就是选择明文攻击的过程。

例如，如果张三访问了李四的计算机，就有可能发生这种攻击。他可以选择一些明文并拦截所创建的密文。当然，他没有密钥，因为密钥通常是嵌在发送方使用的软件当中的。这种攻击很容易执行，但是却不太可能发生。

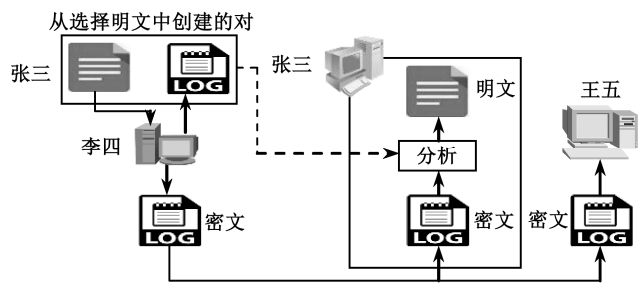


图 6-20 选择明文攻击的过程

4. 选择密文攻击

选择密文攻击和选择明文攻击是相似的，除非张三选择一些密文解密后组成密文/明文对。如果张三访问了王五的计算机，这种攻击就会发生。如图 6-21 所示就是选择密文攻击的过程。

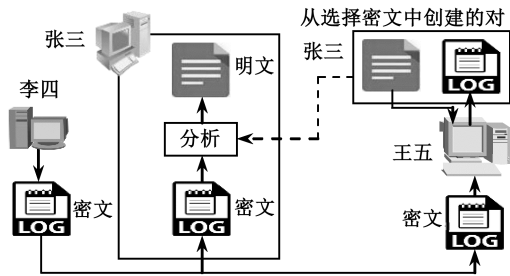


图 6-21 选择密文攻击的过程

6.3 网络空间进攻中的作战战法

网络空间进攻中的作战战法是指在网络空间进攻性作战过程中所采用的作战模式、谋略、战略战术和方法。灵活运用战法，是在网络空间作战中实现以劣胜优的根本途径。根据网络空间作战特点和敌我双方的作战能力及特长，下面介绍一些主要的网络空间进攻中可采取的战法。

6.3.1 网络空间进攻作战的主要模式

从网络空间作战的进攻模式来看，主要有三种：体系破坏、信息误导和综合破坏。

## 1. 体系破坏模式

体系破坏模式通常采用发送计算机病毒、逻辑炸弹等方法，利用系统的软硬件等各方面的漏洞，侵入敌方系统，获取系统访问权限和控制权，破坏敌方计算机与网络系统体系，造成敌方指挥控制系统的瘫痪。任何网络都可以抽象为点与线的编织。网络的点可分为三类：客户机、服务器和网流控制与管理设备（包括网关、路由器和交换机等）。从网络进攻的角度看，所有的点都是网络潜在的威胁，经过刻意地组织就可以成为对网络发动攻击的大规模毁灭性武器。通过向敌信息系统发送大量的无用数据包和电子邮件或输送破坏性程序，使其网络系统堵塞、过载而崩溃，主要手段有 E-mail 炸弹、输入蠕虫等。在 2000 年 2 月全球的“黑客战”中，曾有上百台机器被组织起来，其攻击比特流量超过了 10 亿比特/秒，以致“雅虎”这样的巨型网站也整整瘫痪 3 小时。而超过 1 万亿比特/秒能量级的重型炸弹，足可以在网络上掀起海啸般的巨大比特洪流，所到之处，网络将一片死寂。

## 2. 信息误导模式

向敌计算机与网络系统传输假情报，改变敌网络系统功能，可对敌决策与指挥控制产生信息误导和流程误导。渗透性攻击是其常见的“破网术”，它运用信息截流—信息变质—信息输出的程序，采取“病毒”感染、信息欺骗等手段，破坏敌方的信息系统或使敌方获取的信息变质。当战场网络开始工作，使用无线信道传输信息时，分布在太空、空中、海上、地面的网络侦察设备就可以截获信息，并做相关的解密处理。在掌握其网络协议及密码后，就可以以无线的方式进入敌方的战场网络之中，实施网络窃密或病毒攻击行动。例如，在科索沃战争中，美军就曾通过截取的通信链路把制造的假雷达图像插入南联盟防空计算机网络系统中，致使南联盟防空系统陷于瘫痪。

## 3. 综合破坏模式

综合利用体系破坏和信息误导，并与其他信息作战模式结合，对敌指挥控制系统造成多重杀伤功效，如肢解性攻击，即着眼信息网络的拓扑结构，破坏其关键网络节点，如防空系统的预警雷达，通信系统的枢纽等。美国陆军从 1994 年开始实施的数字化部队建设，其目的是通过网络把战场上的单兵、单个作战平台和战场指挥控制系统联为一体，形成一个巨型的战场网络系统。鉴于战场网络的高度保密性，通常与互联网物理隔绝；鉴于战场的高度机动性和无线传输特性，就可以对战场网络实施有效攻击。如果无法破解网络协议和密码，利用强烈的干扰信号去压制战场网络无线信道，也可以达到扰乱战场网络正常工作的目的。如果战场网络系统事先已被预埋了病毒，就可以以不同的方式随时触发病毒。当然，对战场网络的破坏还可以采取火力打击、兵力袭击等传统手段。

### 6.3.2 网络空间舆论进攻战法

网络空间舆论进攻战法是指利用高性能的网络舆论传播平台，对敌主动进行舆论攻



心,直指目标受众的“认知系统”,有计划地向受众传递经过选择的信息和材料,从而影响受众的情感、动机、主观判断和行为选择,主导新闻舆论、影响民意归属,达到瓦解其民心士气的目的,从而改变双方整体力量对比的行动。网络空间舆论作战的强大影响力是基于网络媒体的强大功能而实现的,其本质在于争夺、控制网络空间舆论传播权。可以说,在未来信息化战争中,谁取得网络媒体的控制权,谁就取得信息权和舆论主导权。

新闻网站和登录新闻的门户网站具备传播主体多元化、传播过程即时化、传播方式立体化、传播内容延展性、传播关系交互性等特点。这些特点决定了网络媒体在信息覆盖的广度和深度,信息传播的速度、密度和强度等方面具有传统媒体(报纸、广播、电视)无法比拟的优势,为敌对双方进行舆论较量提供了广阔的舞台。

网络空间舆论进攻战法的选择和运用,由作战目的、战场敌我态势、网络舆论战对象特点、网络信息技术水平和国际环境等因素决定。通过分析近年来高技术战争中的典型战法可以看出,网络空间舆论进攻战法主要有4种,下面分别进行介绍。

### 1. 先声夺网

先声夺网就是要始终把握网络舆论斗争的先机,正确分析和科学预测网上舆情的变化,对作战各阶段的重要行动、民众关注的重大事件和可能被敌利用的敏感问题,抢先发布信息,及时发表网络评论,主动引导网络舆论。坚持先敌而动,先发制人,快速反应,夺取和保持网上舆论主导权。战法的奥妙就在于把握主动权。在战争状态下,首先必须强化网络舆论的进攻意识,集合网络传播的诸多优势,抢占舆论高地,对外体现出强烈的战略威慑。根据心理学的注意理论、首因效应、晕轮效应、投射效应等,人们首次接受的信息,往往对其后来关于事物的认知和行为具有较大的影响力,产生先入为主、不易改变的持久性作用。因此先声夺网是网络舆论战的重要战法。

(1) 抢先发布网络信息。它是指在出现热点战事新闻的时候,网络空间舆论作战实施者要迅速做出正确反应,以发布网络新闻信息的方式,抢先把握制造舆论的先机,赢得网络舆论战的制高点。要做到这一点,一是要关注战时重大、敏感的新闻事件;二是要抢先(领先)于各方面势力做出反应;三是正确发布的网络信息要符合己方舆论战宣传口径,要做到严谨缜密、滴水不漏,不能落人口实。

(2) 及时发表网络评论。它是指在战时出现突发事件时,网络空间舆论作战实施者要在第一时间做出反应,利用有利于己方作战行动的网络评论及专家意见,把握战时网络舆论方向。要做到这一点,一是要拥有自己的具有战时特色的评论栏目和一批评论专家;二是要及时跟踪新闻言论并加以评论;三是评论的内容要能迎合网络空间舆论作战对象的需求。

(3) 实时交互引导舆论。网络空间舆论战中的交互性,一方面是指网络空间舆论作战对象有更多自主权,他们可以自己决定何时何地以何种方式获得何种信息;另一方面指舆论作战实施者对网络空间舆论战对象的影响更加直接,可以通过多种方式,如电子论坛讨论、聊天室交谈、电子邮件往来和网上舆情调查等方式加强与网络空间舆论作战对象之间的联系。实时交互引导舆论,就是利用网络媒介实时交互的特点,在网络空间舆论作战中进行渗透引导,争取人心,把事实说服力、人道感染力、文化影响力和权威人士公信力

融入实时交互的战时网络舆论宣传中，在充分分析、了解网络空间舆论战对象思想情况、心理状态的基础上，影响和争取人心。做好战时实时交互引导舆论，一是要尊重网络空间舆论战对象意见自主性，保证网络空间舆论战对象的话语权；二是对所提供的实时交互渠道、公共言论区要进行有效的组织和管理；三是对网络实时交互可能带来各种意见的纷争，导致舆论的情绪化、分散化，以及负向舆论形成等问题，要注意因势利导。

## 2. 营造网络空间舆论优势

营造网络空间舆论优势就是要在网上集中造势，形成规模，根据作战意图，围绕特定主题，在一定时段内，通过网络进行多波次、高强度的连续突出宣传，营造强大舆论声势。

(1) 多媒体造势。网络空间舆论作战融合多种传播形式为一体，具有信息传播方式多媒体的特点。报纸通过纸质媒介利用文字图片传递新闻，广播以声音发送信息，电视借助影像播放节目。网络新闻媒体则兼容文字、图表、声音、图片、动画、影像等多种传播手段保存信息、表现信息、发送信息。网络空间舆论作战实施者利用网络媒体的这种特点增强网络舆论战效果，营造网络舆论优势的方法，就叫多媒体造势。要做到这一点，一是综合运用多种媒体表现方式使得战事报道生动形象。如科索沃战争期间，美国国防部的官方网站为向世界炫耀其准确的轰炸效果，以达到威慑对方、鼓励己方的目的，就采用了文字、图片、视频等多种媒体表现方式；二是各种媒体形式必须围绕同一个战争主题展开，才会营造最大的网络空间舆论优势；三是要充分发挥各种媒介形式的优势，实现不同方面信息的互补；四是多媒体信息在形式、技术上要便于网络空间舆论作战对象浏览阅读。

(2) 多波次高强度突出宣传。也就是说，在网络空间舆论作战中要集中造势，形成规模。要根据作战意图，围绕特定主题，以“评论员文章”“文章推荐”等网络传播形式进行突出宣传，营造强大舆论声势。一是利用“大众心理”制造“新闻热门”；二是以“评论员文章”“文章推荐”等形式造就战时“舆论中心”。

(3) 与传统媒体相结合。也就是说，网络空间舆论作战不能忽视传统的舆论战形式。网络媒体与传统媒体互有专长。要做到这一点，一是要理解网络空间舆论作战是信息化战争时代舆论战的重要形式，但不是唯一形式；二是要营造网络舆论优势，不同媒介之间要合作互动；三是要根据具体的国情、军情和敌我双方的特点综合运用不同的舆论战形式。

## 3. 网络空间舆论渗透

网络空间舆论渗透是指网络空间舆论作战实施者要把事实说服力、人道感染力和权威人士公信力等，融入网络空间舆论作战中，从而潜移默化地影响和争取作战对象。

(1) 巧用“事实”进行渗透。就是说，一方面网络空间舆论作战的内容要遵循新闻真实性的原则，要用“事实”说话，让网络空间舆论作战对象相信作战内容的真实性。如果一味地追求“暂时效应”，最终会损害网络空间舆论作战实施者与网络媒体的信誉，从而损害网络空间舆论作战的“最优效应”。另一方面要有技巧地将“事实”重组、排列，使网络空间舆论作战实施者的意图在不违背“事实”的情况下得到最好表达，从而潜移默化地影响和争取作战对象。一是强调于己有利的“事实”。将于己有利的“事实”，在网上给

予浓墨重彩、高强度地强调和集中报道。二是规避于己不利的“事实”。对于不利于作战的消息，可延迟在网上发布或予以回避和限制知情范围，或者让于己不利的“事实”湮没在其他网络信息中，弱化该“事实”受关注的强度。三是突出对敌不利的“事实”。四是淡化背景，对“事实”作有倾向性的解读。

(2) 发挥“网上舆论领袖”的作用。每个论坛都有自己较为稳定的参与群体，而在这些参与群体中，一些文字表达能力强、分析问题深刻、有独特见解的网民的发言往往影响甚至左右其他网民的看法，并由此引导、控制着整个论坛的舆论方向。这些人就被称为“网上舆论领袖”。一是通过“网上舆论领袖”的阐释，增强网络空间舆论作战内容的可信度。二是让现实权威人士上网，充当“网上舆论领袖”。可以通过网络聊天室等方式，请高级指挥员、军事理论专家与学者等，在网上与公众实时交流战况、相关军事知识，对战事做于己有利的预测与分析。三是制造“网上舆论领袖”，把握网上舆论态势。可让一批网络舆论战人员在网上匿名取得“舆论领袖”的地位，在战时就有争议的问题及时发表评论，捍卫政府、军队的立场，以实现监控网上舆论态势，引领网上舆论走向的目的。

(3) 增强网络空间舆论的人道感染力。这是指在网络空间舆论作战中，结合特定的网络空间舆论作战内容和网络环境，向网络空间舆论作战对象传递一些有人道主义感染力、有说服力的舆论宣传信息，借此拉近作战实施者与对象之间的感情距离，打消网络空间舆论作战对象对网络空间舆论作战实施者的敌意和对网络空间舆论作战内容的抵制。要做到这一点，一是要找出与网络空间舆论作战对象之间的共同点；二是要循序渐进；三是要尽量避免激化对立情绪；四是要悟守“人道主义”宣传基调。任何性质的网络空间舆论作战的根本目的是证明自己战争的正义性，都是高扬人道主义的大旗。例如，像美国在明目张胆地违反国际公约侵略一个主权国家南斯拉夫时，却还始终在网络上宣扬“我们是在惩罚不顾人权灭绝人性的恶魔米洛舍维奇，是在进行一场正义的惩罚战，我们是世界的有功之臣”，而不愿撕下温情脉脉的“人道主义面纱”。

#### 4. 与其他网络作战样式协同

在现代高技术战争中，需要以战略目标为牵引，实现多兵种、多种作战样式的结合，发挥出最大作战功效。网络空间舆论作战往往是同网络战、电子战、网络心理战结合起来实施的。例如美国情报系统不断地向伊拉克国内具有社会影响力的主流阶层发送电子邮件。这些邮件列数了伊拉克总统萨达姆执政20年来的种种“罪状”，并极力劝降这些社会主流人士。巴格达陷落半个月后，美国广播公司驻巴格达的两位记者采访了3名伊军军官，这3名伊军军官承认，美军的舆论战和心理战的确动摇了伊军抵抗的信心。

### 6.3.3 网络虚拟战法

网络虚拟战，是运用以计算机成像、电子显示、语音识别和合成、传感等技术为基础的新兴综合应用技术。在计算机网络空间以虚拟现实的形式实施的网络战，其方法是运用

信息化战场“信息网”上的某一节点，把己方计算机与敌方联网，或战前通过各种途径，将虚拟现实技术成果植入敌方的指挥控制信息系统中，把己方战术佯动的假情报、假决心、假部署传输给敌方，以迷惑敌人，诱敌判断失误；向敌指挥官和士兵发布敌方军官假命令、假指示、假计划，屏蔽或欺骗敌情报系统，以改变敌作战意图，从而使其军事行动陷入混乱；使敌方在三维声、像环境中，看到酷似在真实环境中发生的有利于己方的立体交战图像，以扰乱敌军心，破坏敌士气。

要实施网络虚拟战，要做到以下三点。

### 1. 以虚示虚，引蛇出洞

“以虚示虚”，通常是指在强敌进攻面前，己方力量空虚，却仍然表现出空虚，使敌疑己方之虚为实，害怕己方暗中设有圈套而畏步不前。网络空间作战中的“以虚示虚”是指将信息故意“泄露”给敌方，误导敌攻击己方某一非核心网络或诱饵网络，让其认为进攻得手，同时，己方利用敌害怕暴露其攻击源的心理，对其攻击源的地址进行追踪，及时发布敌重要网络主机地址、攻击源地址或攻击策略，迫使敌减轻或停止对己方核心网络的攻击。

### 2. 以虚示实，迷敌耳目

“以虚示实”，即己方作战力量空虚或弱小，通过某些措施，表现为强大，预有准备；或者不准备采取作战行动时，却故意装作要行动的样子。运用“以虚示实”谋略可以达到影响网络空间舆论作导向、掌握舆论宣传主动权的效果。

一是大幅发布利于己方的新闻报道，邀请有影响的专家、政客利用计算机网络作为媒介，有目的地采用传送虚假信息，误导预定人群目标的方法，降低对方民众的支持率。二是在己方可控制的国内官方网站、访问量较大的民间网站上发布信息，快速反击对己方“不利”的敌方报道，必要时可以过滤甚至摧毁发布“不利”内容的网站。三是在敌方或第三方国家，建立访问量较大的镜像站点，以对方的知识阶层或其他有关阶层展开心理宣传，为战略意图做舆论宣传。

### 3. 以实示虚，请君入瓮

一是网络空间欺骗“示虚”。通过将大量IP地址绑定在己方的某一台（组）计算机上，使敌误认为这一网络空间内存在有价值的目标，增加搜索网络空间工作量，大量消耗敌方网络的资源，使己方真正的网络服务被探测到的可能性大大减小。二是增加敌对我“网络陷阱”的发现概率“示虚”。“网络陷阱”也被称为“蜜罐”。指挥员将“蜜罐”广泛分布到己方网络中，增加“蜜罐”在整个网络中的百分比，故意暴露“蜜罐”的安全弱点以增加其“甜度”，从而牵着对手的“鼻子”逐步进入己方预先设置的“网络陷阱”，而己方则假痴不癫，诱敌上当，使之落入圈套，以估测对方的进攻意图。三是牺牲网络“幕僚”机“示虚”。通过牺牲网络“幕僚”机“舍车保帅”，将进攻者的注意力转向网络僚机，迟滞、延缓敌方突破己网络防御层的速度，可以使己方在预警、保护、检测、响应、恢复和反击的防御周期上赢得时间。

### 6.3.4 以奇制敌取胜战法

#### 1. 选择奇时，奇夺先机

临机设伏出“奇”。网络空间作战武器的使用具有时效性，一般在首次使用时效果最好，被敌发现和采取防御措施后就很难奏效，因而，只能在特定时机使用，让敌猝不及防。例如，科索沃战争中，南联盟黑客首次运用计算机病毒对北约信息网络攻击，使其一度通信中断就是典型的例子。

利用敌心理松懈之时出“奇”。网络进攻一方在进攻方式、进攻时机、进攻区域选择上都有很大余地，可以因时、因地抓住战机发起攻击，而网络防御一方必须长期地监视维护网络。因此，双方的较量不仅是技术上的比拼，更是意志和耐力的较量，利用对方心理上的松懈可以创造以奇制胜的良机。

利用时间差出“奇”。网络对抗存在时间差，这个时间差是某一方发起进攻的时间与另一方的网络防御响应时间之间的时间窗口。就网络防御而言，防御行动一般在对方攻击行动后实施，使受保护的信息网络给进攻者暴露了一个可攻击的时间窗口，初次攻击屡屡奏效。例如，2006年“魔波蠕虫”（利用MS06-040漏洞），其木马攻击均采用了“零日攻击”方式。

#### 2. 夺占奇地，奇乱敌阵

夺占“奇地”，就是在敌人未能预料的目标网络部署己方作战力量或实施攻击、防御行动。信息网络由若干网络节点连接而成。这些节点是信息网络的重心，夺取信息网络的重心就是占据了“奇地”。

随敌应变寻“奇地”。信息网络以软件为基础来实现关键性节点位置的变换，重心很少固定在一定物理空间，网络体系处于不断地变化之中。寻找“奇地”就是随着敌方信息网络重心的变化，在技术上不断调整自己的网络结构；在战术上改变攻击思路，搜寻、找到并夺取敌人的信息网络重心。

分层突破潜入“奇地”。选择敌骨干网络工作站、网关、路由器、数据中心等设备，在获取敌重要核心网络、站点的合法访问权后，由外及内，占据敌方访问量较大的网站作为“奇地”。

飘忽不定占据“奇地”。在敌网络中植入病毒，借助网络流量巨大的特点，使“奇地”的范围扩大，同时在短时间内不停地切换所占据“奇地”的IP地址，使敌难觅己方行踪。

#### 3. 妙用奇器，奇乱敌网

妙用“奇器”的要旨是必须在掌握技术“杀手锏”的基础上攻击对方网络。以新式网

络战武器装备求“奇”。就是针对不同类型的网络研制、发展和创新网络战武器装备。例如，对于不容易渗透的网络，采用反弹式病毒、复合式邮件病毒；对于使用商业技术较多的军事网络，根据运用技术的特征，研究和参考商业技术资料，并将商业网络中不断翻新的网络进攻方式直接运用到这些军用网络中；针对完全物理隔离的网络，可以采用新式的“硬摧毁”的办法，破坏计算机网络基础设施。最近以色列军队开发出一种能隐蔽地发起攻击的病毒武器，这种病毒程序采用特殊的隐形技术，进入敌方系统造成大面积感染。

以旧式网络战武器装备求“奇”。例如，2007年9月18日，德国PC厂商Medion公司交付的10万台笔记本电脑被13年前的老病毒所感染。这些笔记本电脑预装最新版Windows Vista操作系统，并安装了Bullguard杀毒软件，但未能阻止该病毒的攻击。

对网络空间作战武器装备升级改造出“奇”。运用新式或旧式网络战武器装备属于“奇法”中的“正法”，一旦使用，敌方很容易找到对付这些武器的办法。在这些网络战武器的基础上进行改造升级，新旧组合，功能搭配，就可以在短时间内不断变化出某系列的诸多武器，让敌防不胜防。

#### 4. 善用奇法，奇瘫敌网

变中出“奇”。也就是要打破侦察、踩点、攻击或预警、响应、防御等程序化方式，在作战行动中实现攻击方式的多样化，攻击手段的多样化，指挥方式的多样化。如通过第三国或军事战略网络改变攻击点、攻击方向和攻击路线，进行迂回式的“跳板攻击”。

反思维出“奇”。也就是反常使用网络作战力量、作战方法，反常用兵出奇。例如，进攻一方使用非常随机的源IP地址，保护自己不被防御一方发现；对攻击数据包结构采用千变万化的形式，使敌方难以找到攻击流量特征；采用多种攻击并行的形式，加强攻击强度，增加敌方的防御难度；增大更高的发包速率，使攻击特征更加不明显等。

合理冒险出“奇”。网络对抗的本质是攻防双方不断利用网络脆弱性进行的相互博弈。作为攻击方，受防御方网络欺骗和环境影响，在攻击重点、攻击方式、攻击时机选择上存在不确定性，所以攻击方存在被对手发现、反击的风险。作为防御方，受攻击方假象迷惑和环境影响，在防御重点上也存在不确定性，防御方也存在较短时间内被对方攻破网络的风险。所以，不论是处于网络防御或网络进攻地位，必须采用诸多战术手段迷惑对手，合理冒险，快速做出决策，在激烈的网络对抗中占有主动权。

### 6.3.5 破“墙”击要法

破“墙”击要法，是指着眼支撑敌方作战体系平衡的重心，集中精锐力量，首先破坏敌方指挥控制系统的防火墙，而后运用多种手段对敌方核心系统实施高强度软硬攻击，瘫痪敌方指挥控制系统。未来战争中，参战力量的多元性和战场情况的多变性，使作战中的指挥控制决策日益困难，必须利用计算机指挥控制辅助决策系统来帮助其完成作战决策和

指挥。因此,破坏、干扰或摧毁敌方指挥控制系统,对于夺取战场制网络权十分重要。

在网络空间作战中运用破“墙”击要法时,一是全面掌握战场情况特别是敌情。通过掌握情况,指挥员应清楚了支撑敌方计算机网络系统运行的战场信息资源环境,敌方指挥控制系统的结构、指挥控制关系和决策过程。二是把支撑作战体系平衡的重心进行科学分解。作战重心是有层次的,可分为战略重心、战役重心和战术重心。一个高层次重心由若干个下级重心(分支重心)来支撑,在着眼关系敌方总体平衡的全局重心实施攻击的过程中,应首先攻击维系敌全局重心平衡的分支重心。如对敌方核心指挥控制系统实施实体摧毁,必须首先破坏其防空预警系统;对敌核心计算机网络实施攻击,必须首先攻破敌外围防火墙。因此,在全面掌握战场情况的基础上,应根据敌目标的重要程度确定优先打击次序。三是合理使用作战力量并赋予作战任务。在对敌要害目标实施攻击中,应灵活使用“软硬”打击力量,合理赋予作战任务,对使用网络空间攻击手段难以破坏的系统,应使用精确作战和特种作战力量予以摧毁。对精确打击力量难以摧毁的敌计算机系统,应使用网络空间攻击力量予以攻击。同时,做好“软硬”攻击行动的协调,既要确保瘫痪敌指挥控制系统,又要避免重复打击,造成作战能量的无效释放。

### 6.3.6 毁“网”断流法

毁“网”断流法,是指在网络空间作战中,通过破坏敌方网络空间的完整性和一体性,达到破坏敌方各种作战力量和各种作战行动之间有效协调的目的。战争参战力量的多元性和作战行动的复杂性,决定了作战中必然把各种作战行动和各作战集团之间的协调放在首位。而作战协调必须依靠网络将各种作战力量组合成一个整体。因此,网络空间作战要将破坏敌方各种力量之间协调,同时保护对己方各种力量之间的有效协调置于重要地位。

在网络空间作战中运用毁“网”断流法,重点是破坏敌方战略网、战役网和战术网之间、各作战集团网之间的网络连接,使其难以实施有效协调。计算机网络是由若干局域网和广域网组成的,尽管其发展目标是一个无缝的网络,但并不是一个没有层次的网络,在计算机网络的使用上也存在逻辑上的层次区分。各个层次、各个军种和各个作战集团的广域网之间,必须通过通信网络相连接。破坏连接各广域网的通信网络,就能使敌战略级、战役级和战术级之间,各军种及各作战集团之间的指挥信息、协同信息难以有效传输,从而破坏敌协同作战。因此,联合网络作战指挥员应通过网络侦察,明确敌方各种力量的构成及组织指挥体系和相互协同关系,明确敌方是通过何种手段,在何级别或层次组织协同。在此基础上,按照先大后小的顺序,即先是敌方不同国家或不同编制体制的武装力量之间的计算机协同网络,其次是各军(兵)种之间的计算机协同网络,再次是战役级作战兵团的计算机协同网络,最后是战术级作战兵团之间的计算机协同网络,组织力量依次实施攻击。

### 6.3.7 夺“点”控网法

夺“点”控网法，是指在网络空间作战中，通过夺占网络空间的重要站点，控制敌方部分网络，在敌方还未觉察并关闭该站点时，对敌方网络空间实施高强度攻击，造成敌方网络空间全局或局部混乱。这种战法着眼于网络空间的一体性和资源共享性特征，在夺占敌方某一站点后，由此及彼，迅速扩大战果。

在网络空间作战中运用夺“点”控网法，在组织周密细致的网络侦察时，应首先选择敌方大型计算机工作站、网关、路由器、交换机、集线器、数据库等设备、设施；其次选择较大规模武器系统的指挥控制系统，如战区雷达预警系统；最后再分析小型网站、单机或武器的自动控制系统。同时，组织力量破解敌方网络站点的网关、密钥和安全防火墙。在此基础上，针对敌方重要的核心网络、站点的防护严密、安全措施和反入侵手段的完善情况，采用由外及内，首先攻占敌方外围站点，取得合法访问权限后，迅速采取网络进攻手段，逐层突破，达到网络攻击的目的。

### 6.3.8 断“源”瘫网法

断“源”瘫网法，是指在网络空间作战中，通过攻击支撑敌方网络空间运行的通信、电力和战略、战役纵深的网络及其基础设施，使敌方网络空间失去可靠的支撑，导致其运转不灵，甚至瘫痪。未来战争中，在依靠网络将战场前、后方的网络连为一体，使前、后方界限模糊的同时，也存在前沿部署的各级网络必须依靠战略纵深、战役纵深的网络和信息基础设施的支撑。因此，通过运用断“源”瘫网法，能较好地达到网络作战的目的。

在网络空间作战中运用断“源”瘫网法，可采取：一是攻击敌方战略纵深和战役纵深的网络。在联合作战开始之前或稍后，组织软硬攻击力量对敌方通信枢纽、电力网和电厂等实施攻击，断“源”瘫网，使敌方网络失去能源和动力的支撑，直至瘫痪。二是计算机系统大大提高了武器系统的效能，但也带来了一个致命的弱点，一旦计算机系统遭到破坏，武器就变成一堆废铁。近期的局部战争表明，在侦察预警系统的支持下，首先使用远程武器实施攻击是敌方首选手段。因此，攻击敌方预警系统和远程武器的计算机系统可以极大地削弱敌方的威胁。

### 6.3.9 先“动”后“静”法

先“动”后“静”法，是指在网络空间作战中，在作战目标的选择上应着眼敌方网络的关键节点，先打击机动目标，后打击静止目标，达到网络空间作战的目的。在未来战争



中, 各类信息系统将向高机动、小型化、分布式的方向发展。同时, 固定信息系统需要依靠机动信息系统来实现战场的无缝连接, 构成一体化的信息系统。同时, 通常情况下静止目标战前易于监控, 作战中可运用多种手段实施有效打击, 而机动目标则难以捕捉和打击。因此, 在网络空间作战中抓住敌方机动信息目标实施有重点的打击, 就抓住了网络作战的关键。

在网络空间作战中运用先“动”后“静”战法, 可采取: 一是攻击敌方重要机动平台上的网络系统。如对敌方空中预警飞机、航空母舰、机动导弹发射系统等对己方威胁较大的系统, 必须给予有效的攻击。二是利用机动信息系统传输信道的开放性实施攻击。机动信息系统必然要使用空中信道进行信息和数据的传输与交换, 无线信道的开放性为敌方入侵敌方的网络提供了十分便利的条件。通过对无线信号的分析, 可以发现敌方网络系统的基本结构、数据特征、地址分配等信息。同时, 开放的信道既为网络侦察提供了便利条件, 也为组织实施对敌方网络实施无线注入病毒攻击提供途径。三是利用机动信息系统中断或恢复联络频繁的特点实施攻击。由于机动信息系统要经常处于高度的机动状态, 必然易受干扰和破坏, 使得机动信息系统与其他系统的联系遭到破坏。在敌方网络中断或恢复的过程中, 可以利用多种技术手段渗透到敌方的网络系统中, 从而打开敌方网络的突破口。

#### 6.3.10 局部造优法

局部造优法, 是指网络空间作战指挥员以灵活的作战指导, 突然地集中力量于关键的时域、频域和区域, 形成对敌方的局部优势。集中兵力是一条军事通则, 特别对在网络空间作战中处于劣势的一方, 尤其需要灵活地运用集中兵力战法, 依据作战计划, 在关键的时机和方向形成局部优势, 对敌方实施高强度攻击, 由点及线, 由线及网, 达到“以点断脉”, “以脉破网”的目的。

在网络空间作战中运用局部造优法, 可采取: 一是集中运用网络空间作战力量。联合网络作战力量的构成是多元的, 只有通过科学规划、周密安排, 才能使各种力量形成合力, 在局部形成对敌方网络空间作战的优势。二是集中运用网络空间作战手段。在组织进攻时, 要针对敌方网络空间系统的特点, 善于发现敌方网络空间的弱点, 选择有效的手段实施。在组织网络空间防御时, 要组织多级多样的安全防护措施, 通过多种手段, 层层设防, 从整体上提高网络空间防护能力。

#### 6.3.11 网电一体进攻战法

随着无线网络的发展, 网络空间与电磁空间逐渐融为一体。网电一体进攻战实现了电

子战、网络战、硬摧毁等多种攻击手段的高度融合。根据“网电一体战”模型，如图 6-22 所示，（分）节点是各级指挥部和信息交汇点，电子战的攻击点主要在各传感器、作战单位和信息传输通道等信息获取、传输环节，而网络战的攻击点主要在各（分）节点的信息处理、利用环节。在利用传统电子攻击手段对敌方信息系统和武器装备等实施实体摧毁的同时，应加强电子战和网络战的综合运用、密切协同，形成“网电一体”的攻击手段，全面打击敌方信息系统的各个环节，形成信息优势，夺取战争的胜利。

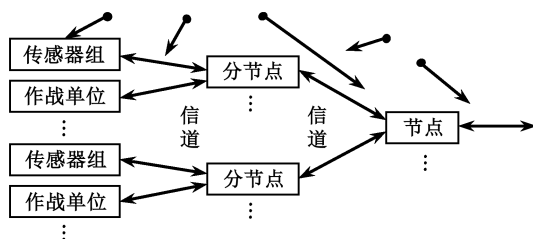


图 6-22 “网电一体战”模型

### 1. 实施精确打击，毁节破网

战场信息网络是由遥感侦察系统、通信传递系统、处理决策系统、部队行动和武器打击系统、保障供应系统五大系统组成的整体运行的网络。这五大系统中的每一个系统，又由若干子系统组成。这些作为节点的系统都可成为军队所选择的打击目标。一旦对敌方遥感侦察系统、通信枢纽、计算机控制中心等网络节点目标实施多点精确打击，就能使敌方信息网络系统无法正常运转。海湾战争初期，美空军在伊拉克选定了 78 个网络节点，战争打响才 28 分钟，就切断了伊拉克军方指挥部同部队的联系。

在实施精确打击时，军队使用巡航导弹、反辐射导弹、精确制导炸弹等信息化弹药或常规弹药，在预先侦察的基础上，重点打击敌方指挥控制中心、通信枢纽、雷达站、计算机网络节点，以及其他重要情报信息侦察系统和平台，摧毁、破坏敌方信息作战系统；或派遣特种部队，秘密渗入敌方，对敌方信息系统的要害目标和关键环节实施重点破坏；可以使用高功率微波或激光武器等高技术武器装备攻击敌方计算机、通信网络节点，摧毁和杀伤敌方信息系统的电子设备与人员，瘫痪敌方战役信息系统。还可以采取釜底抽薪的“断粮”战术，使用“石墨炸弹”，大规模破坏敌方供电系统，使敌方信息网络中的电子设施得不到电能供应而形同虚设，处于瘫痪状态，从根本上破坏、摧毁敌方信息网络系统。

### 2. 实施多种干扰，错节乱网

电子干扰是军队信息进攻的重要手段。在联合战役重要作战阶段、主要作战方向和重点地区，军队可充分发挥电子战的优势，通过雷达、通信、光电等各种干扰形式对敌方要害电子目标和空间信道实施有源或无源、瞄准或阻塞式干扰，破坏敌方通信线路和节点，扰乱其信息网络的正常运行，降低其信息传输能力。也可以借鉴科索沃战争中以美国为首的北约部队对南联盟成功实施网络战的经验，使用一次性电子干扰机和电磁脉冲炸弹。一次性电子干扰机由飞机、导弹投掷到战场纵深内，落地后自动伸出天线，对敌方信息网络

系统中的电子设备进行全频段的阻塞式干扰,干扰后能定时自毁,令敌方摸不着头脑,遭受了干扰还不知道干扰源在哪里。电磁脉冲炸弹能将爆炸的化学能转变为电磁能,产生出强大的电磁脉冲,轻者能将距爆心一定距离范围内的信息网络中的电子元器件击坏,重者将其烧毁化为一缕青烟。也可以使用微波炸弹,在瞬间辐射强大的微波能量,通过信息网络设施的多种入口(如天线、电源线、传输线等)进入网络,微波所产生感应电荷和电流,改变网络线路某些元器件的工作状态,造成电路功能紊乱,传输的信号产生误码和错乱,甚至使整个网络失去控制。微波炸弹可安装瞬发引信由飞机直接投掷,也可安装定时引信由特工人员进行秘密布设,攻击的目标主要是网络中心、指挥枢纽和各种网络节点等重要信息战部位。

### 3. 实施病毒注入,传染瘫网

以计算机病毒为代表的信息武器将成为新一代的战略威慑性武器。由于计算机病毒武器的形态主要是程序,构成简单、造价低、使用方便。因此,计算机病毒攻击对于网络的破坏将更直接、更有效、更现实。在海湾战争中,美军运用初级计算机病毒武器成功地攻击了伊拉克的指挥中心,使伊拉克耗费巨资建立起来的防空网络系统失去作用。

计算机病毒武器“侵入”的方法多种多样,主要有无线电空间注入、设备研制期注入、有线电网/节点注入等。运用计算机病毒攻击手段实施电子战的手段一旦成功,即可使敌方赖以生存的网络变为其走向失败的“导火索”。

在实施计算机病毒攻击时,还可以使用一种新型的计算机病毒武器——“逻辑炸弹”,作战时,将其输入敌方网络。病毒能在预定的时间内“苏醒”过来,进行“爆炸性”的繁衍,大量的病毒迅速“吞噬”计算机中的各种数据和信息,使计算机网络处于混乱不堪的无序状态之中,整个系统将失去控制。

### 4. 实施“阻塞”攻击,超载废网

作战指挥是通过控制信息流去控制战场上的人流、物流、能量流的流向、流量和有序流动。而计算机储存和网上信息流动,均有一定的容量限制,超过容量限定指标后,就会造成信息流动的不畅。因此,可通过有意向敌方信息网络倾泻虚假信息、过时信息,制造“信息洪流”,阻塞、挤占敌方信息信道,使其无法及时有效地传输和处理所需信息,从而使敌方好网变废网,有网不能用。这种手段就叫“阻塞”攻击,它是“破网术”的一个重要手段。实施阻塞攻击的主要方法有:运用 Ping 命令向敌方信息系统发送 E-mail 炸弹,输入蠕虫程序,施放“梅莉莎”“疯牛”“幸福 99”等计算机病毒。通过这些方法,对敌方网络系统实施高密度的“电子轰炸”,致使敌方信息网络严重超载,通信阻塞。同时还可采取在发送的电子邮件中隐藏形形色色的计算机病毒,使敌方网站处理这些“毒瘤”而花费大量时间,有的甚至根本无法破解,从而使整个网络系统处于一种“忙乱”状态,形同虚设。

### 5. 实施“黑客”攻击,渗透控网

在平时和未来的信息作战中应充分认识到“黑客”的重要作用,应把具有高科技手段

和精通计算机网络技术的“黑客”重点培养使用，为军队夺取制信息权服务。“黑客”们战斗在看不见的网络系统内，凭借自己的高超技术，侵入敌方指挥网络系统，随意浏览、窃取、删改有关数据，或者输入假命令、假情报，破坏敌方整个作战自动化指挥系统，使其做出错误的决策；通过无线注入、预先设伏、有线网络传播等途径实施计算机网络病毒战，瘫痪对方网络；运用各种手段施放计算机病毒直接攻击，摧毁敌方技术武器系统；同时还可以渗透到敌方的金融、交通、电力、航空、广播电视、政府等网络系统，用各种手段破坏这些重要网络系统，搞乱敌方国政治、经济和社会生活，造成社会动荡，从而使敌方无心应战，达到“不战而屈人之兵”的目的。

### 6.3.12 网络空间进攻的实施方法

#### 1. 全面撒网，普遍排查

这是一种大面积扫描主机的方法，主要用于对情况不明的网段进行扫描。该方法也是其他战法运用的基础。通常针对不同的操作系统和情报需求，使用不同途径的扫描工具进行检测。同时，根据网络中不断涌现的新系统、新技术所带来的新安全漏洞，扩充扫描工具的检测方法和手段，并同时建立目标数据库。

#### 2. 分门别类，重点监控

计算机网络结构复杂，主机众多，但并非所有的主机都是侦察重点，因此，必须抓住重点主机、关键节点、主流操作系统等要害目标实施严密的侦察监控。同时，建立重点网络目标库，对这些目标采取定期或不定期的扫描，跟踪其系统漏洞的修补情况，随时掌握其安全状况的变化，为实施网络攻击提供依据。

#### 3. 隐藏入侵，借敌方之势

这种方法是将“跳板机”设置成代理服务器，并通过代理服务器扫描侦察对方网络目标。“跳板机”一般是对方没有设防或安全防护级别较差、易被己方控制的主机。“跳板机”一旦被己方控制，就可以远程操作该主机，完成代理服务器的设置，利用其合法身份可以进入对方网络而不易引起怀疑。通常要建立“跳板机”库，对“跳板机”资源进行管理，而且要严格控制使用“跳板机”，随着对方漏洞的修补，“跳板机”也会发生变化，因此，“跳板机”库要经常更新。

#### 4. 快速渗透，交互感染

这种方法主要是攻其一点，掌握全局，在网络空间作战力量有限情况下，可控制对方大量主机，达到以少取多的效果。如“蠕虫”是一类很好的可快速渗透和感染的程序，可以在网络上不同主机间传播，而无须修改目标主机上其他程序。在网络中“蠕虫”秘密地

传输，不断复制自己并传送到各处，收集包含密码或文件在内的信息，发给己方。

如此反复循环，就可以在短时间内感染大量主机，被感染主机的信息就会在己方掌握之中，为进一步侦察和攻击提供资料。

### 5. 明修栈道，暗度陈仓

这种方法主要利用对方机器的漏洞上传木马程序，木马程序与己方主机进行通信，从而达到控制对方机器的目的。这种方法主要用于长期控守对方主机，从而获取更多信息。在实际侦察中，拥有一定数量能长期控制、为己方所有的对方主机是很重要的，利用它设置成代理服务器。因此，上传木马至部分具有严重安全弱点的主机，并利用各种远程自启动技术激活木马程序，秘密监视网络信息，就可以长期掌握这些主机的控制权。

### 6. 多点切入，迂回攻击

有时某个目标主机表面上看似没有任何漏洞，难以直接入侵。这种情况下，可以借助一些与其有联系的机器，这些机器多数是维护目标服务器的机器或目标服务器的信任友机，然后分析清楚其网络结构，根据网络的拓扑结构，利用目标主机对友机的信任和授权，一步步逼近目标主机，最终达到控制和攻击目标主机的目的。

### 7. 选时避敌方，乘虚而入

这种方法主要指选择合适的时机进行侦察。计算机网络管理是有规律的，同样是有许多不可避免的薄弱环节。通过对对方计算机网络的长期监控可以发现，管理员一般在深夜容易疲劳，疏于防范，放松警惕。这就是入侵的最佳机会，此时进行侦察，不易被发现，可大大增强侦察和设伏行动的隐蔽性。

### 8. 综合分析，扩散运用

网络对抗侦察，要充分考虑各种因素，综合运用多种侦察方法，从而获取最好的效果。由于网络系统种类繁多，体系结构各异，人为因素和管理漏洞在所难免，加之各种网络对抗侦察手段都有各自的优点，因而对敌方网络系统的侦察，应使用不同的手段和措施。只有针对敌方信息系统的实际特点，灵活采用多种侦察方式和手段，才能取得良好的效果。






# 第 7 章

## 防御性网络空间作战

网络空间作战防御已成为世界范围内普遍关注的热门话题。在实施网络空间进攻作战，夺取网络制信息权的同时，保持己方网络空间的正常运转和可靠地发挥战斗力就显得同样的重要。正如军事专家指出的那样：积极的网络空间防御与积极的网络空间进攻有着同样的制胜价值。加强网络空间防御能力建设，认清网络空间面临的安全威胁，掌握网络空间防御作战的理论、技术与方法，了解网络作战防御过程，并采取强有力的作战策略，构建网络空间防御体系是关乎国家安全、社会发展、民族兴亡、百姓生命财产安全的重大战略问题，对打赢网络空间战争具有十分重要的现实意义。我们必须警钟长鸣，奋力前行，打出一套涵盖基础理论、核心技术、方法手段、体系架构、基础设施、保障措施的网络空间防御“组合拳”。

### 7.1 网络空间作战防御基础



#### 7.1.1 网络空间作战防御的概念与分类

网络空间作战防御包括在敌方攻击前、攻击过程中，以及攻击后所采取的旨在保持、

保护、监视、侦查、分析、响应、恢复，以及重建己方网络空间能力而采取的介入控制、安全技术手段、活动、措施和军事行动，包括摧毁敌方打击力量、降低其作战效能、网络空间攻击缓解、生存抗毁能力提高、攻击特性分析、脆弱性探测与响应、数据和电子系统保护，以及电磁防护与基础设施保护等。也就是说，要针对敌方的网络进攻行为，对己方的网络系统和设备进行防护，不让敌方通过非法途径访问和侵入网络系统来破坏己方的网络设备系统、主机系统、数据库和应用系统，削弱和降低己方网络空间的作战效能，或造成己方网络的瘫痪，进而使己方失去战斗力。从另一个角度来说，就是要保护信息网络系统的软硬件及其系统中的数据，使其在遭受偶然的或恶意的攻击时而不被破坏、更改、泄露，系统能连续可靠地运行，网络服务不中断。即防止信息网络本身及其采集、加工、存储、传输的信息数据被故意或偶然地非授权泄露、更改、破坏或使信息被非法辨认、控制，保障网络信息的保密性、完整性、可用性、认证性、可控性、不可抵赖性等。

网络空间防御是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。它是保证己方网络系统正常发挥战斗力，保证网络运行系统安全、网上信息系统安全、网上数据传输安全、网上信息内容安全、物理安全、网络结构安全、管理安全和服务安全必不可少的重要途径。

由于网络空间安全的威胁来自方方面面，因此我们不仅要防止来自外部的进攻，还必须对网上的邻居进行防范；不仅要提防恶意的攻击，还必须加强对无恶意入侵的防护。另外，威胁到网络安全的还有其他一些非常规的因素，比如“单纯性电子干扰”、各种物理干扰、通信线路的开放、专业情报人员的刺探、拥有特权的系统管理人员的不负责任等。这些都对网络安全造成了影响，并加大了防御的难度。

随着网络迅速蔓延，发展的势头很难预测和控制，对破坏的程度难以评估和预测。因此，网络防护的难度大于网络攻击，这是因为有效的网络防护必须能够应对所有的网络攻击，网络攻击只要成功一次，就意味着所有网络防护手段的失效。网络攻击实施更容易、发起速度更快、技术和手段变化更多、所需代价较之网络防护也更低。基于这种攻防之间的不对称性，必须建立功能一体的纵深防护体系。

从内容上讲，网络空间防御可分为网络设备的防御、网络通信的防御、网络软件系统的防御和网络服务的防御。

从方法上讲，网络空间防御可分为被动防御和主动防御。通常，网络空间防御从作战应用上讲，总是处于被动状态，但在方法策略上经常可采用一些主动措施来对付攻击。被动防御包括对信息的加密、对访问进行控制和认证、病毒的防范、使用代理访问和防火墙、对通过的网络信息进行过滤、关闭不必要的服务、寻找漏洞并修补等方面。这些措施一般在网络建设和使用过程中进行规划设置，逐步完善。主动防御包括主动对网上主机进行扫描、实时检测网上的入侵、设置网络陷阱捕捉攻击者、对网络攻击者的跟踪和反攻击，设置大量佯动网站来掩护工作网站等。这些手段虽然有主动的方面，但仍然是比较盲目的，因为己方很难知道敌人什么时候进攻，不过比起静态的被动防御更具有对抗性。

目前，人们在网络空间防御方面开发的技术和工具大体上可以分为三类，分别为预防技术、检测技术和响应技术。



7.1.2 网络空间安全防御系统的功能体系

网络空间安全防御系统的功能体系如图 7-1 所示。网络空间安全防御系统分别从网络安全、主机安全、数据安全、应用安全、安全管理、安全认证、容灾备份、应急处置和最低限度保障等方面提供安全功能。

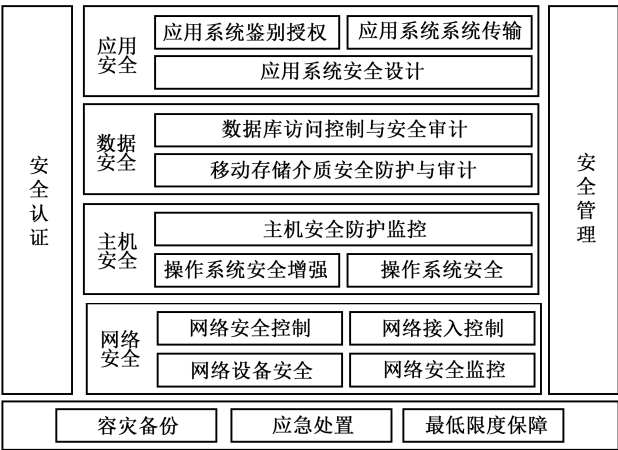


图 7-1 网络空间安全防御系统的功能体系

其中，网络安全包括网络安全控制、接入控制、设备安全 and 安全监控，提供网络隔离、传输加密、网络监控、网络防病毒、网络安全认证等安全功能；主机安全主要包括主机安全防护监控、操作系统安全及安全增强，提供用户安全管理、终端防护、数据库安全、操作系统安全、安全漏洞扫描等安全功能；应用安全主要包括应用系统的鉴别授权、系统传输和安全设计，提供应用安全管理、应用安全认证、信息防篡改、应用系统鉴别授权等应用安全功能；数据安全主要包括数据库访问控制与安全审计和移动存储介质安全防护与审计，提供数据访问控制、数据存储保护和数据备份恢复等安全功能；安全管理主要依托由指挥所、网络节点和各级安全防护中心安全管理系统构成网络的安全管理体系来实现；网络接入控制设备将基于数字证书的认证技术和基于属性证书的授权技术相结合，对所有接入网络的用户身份进行认证，只有经过认证并授权的用户才允许接入网络，并对用户使用网络资源的行为进行监控和审计，以确保网络资源不被非法利用。

7.1.3 网络信息安全防御的基本属性与机制

1. 基本属性

网络信息安全防御的基本属性主要表现在 5 个方面：机密性、完整性、可用性、不可

否认性和可控性。

### 1) 机密性 (Confidentiality)

网络信息的机密性是指确保只有那些被授予特定权限的人才能够访问到信息。网络信息的机密性依据信息被允许访问对象的多少而不同,所有人员都可以访问的信息为公开信息;需要限制访问的信息为敏感信息或秘密信息;根据信息的重要程度和保密要求将信息分为不同密级。例如,军队内部文件一般分为秘密、机密和绝密 3 个等级,已授权用户根据所授予的操作权限可以对保密信息进行操作。有的用户只可以读取信息;有的用户既可以进行读操作又可以进行写操作。

网络信息的机密性主要通过防侦听、防辐射、信息加密、物理保密、身份认证、访问控制和安全通信协议技术来保证。

### 2) 完整性 (Integrity)

完整性是指信息未经授权不能进行改变的特性,涉及信息和处理方法的正确性和完整性。信息完整性一方面是指在使用、传输、存储信息的过程中保持不被偶然或蓄意地删除、篡改、伪造、乱序、重放、插入和丢失信息等现象;另一方面是指信息处理的方法的正确性,执行不正当的操作,有可能造成重要文件的丢失,甚至整个系统的瘫痪。完整性是网络信息系统面向用户的安全性能,要求保持信息的原样,即信息的正确生成、存储和传输。信息的完整性主要通过安全协议、纠错码、密码校验、数字签名、公证、报文摘要和加密技术来保证。

影响网络信息完整性的主要因素有设备故障、误码(传输、处理和存储过程中产生的误码,稳定度和精度降低造成的误码,各种干扰源造成的误码)、人为攻击、计算机病毒等。

### 3) 可用性 (Availability)

网络信息的可用性是指确保那些已被授权的用户在他们需要的时候,确实可以访问得到所需要的信息。即信息及相关的信息资产在授权人需要的时候,可以立即获得。例如,通信线路中断故障、网络的拥堵会造成信息在一段时间内不可用,影响正常的业务运营,这是信息可用性的破坏。提供信息的系统必须能适当地承受攻击并在失败时恢复。网络信息的可用性主要通过实时的备份与恢复技术来保证。

网络信息系统的可用性测度主要有 3 种:抗毁性、生存性和有效性。网络信息的抗毁性是指当网络中出现确定性或随机性故障时,网络能维持或恢复其性能到一个可接受程度的能力。生存性是指网络信息及其信息服务系统在攻击、故障和意外事故已发生的情况下,在限定时间内完成使命的能力。有效性则是一种基于业务性能的可靠性,是指在网络信息部件失效的情况下,满足业务性能要求的程度。

对网络可用性的损害主要来自人为操作错误、系统软件或应用软件缺陷、硬件损毁、电脑病毒、黑客攻击、突然断电、意外宕机、自然灾害等诸多因素,这些需要不同的安全防御技术来应对。这些技术主要有 3 种:可自愈的自适应路由协议、数据备份与灾难恢复

技术、入侵容忍技术。

#### 4) 不可否认性 (Non repudiation)

信息的不可否认性也称抗抵赖性、不可抵赖性,它是传统的不可否认需求在信息社会的延伸。人类社会的各种商务和政务行为是建立在信任的基础上的,传统的公章、印戳、签名等手段便是实现不可否认性的主要机制,信息的不可否认性与此相同,也是防止实体否认其已经发生的行为。信息的不可否认性分为原发不可否认(也称原发抗抵赖)和接收不可否认(接收抗抵赖),原发不可否认用于防止发送者否认自己已发送的数据和数据内容;接收不可否认防止接收者否认已接收过的数据和数据内容。实现不可否认性的技术手段一般有数字证书和数字签名。网络信息的不可否认性主要通过身份认证技术来保证,这些身份认证技术包括数字签名、数字证书、集成电路(IC, Integrated Circuit)卡或 USBkey(一种 USB 接口的硬件设备)令牌、指纹、视网膜、掌形、脸形等。

#### 5) 可控性 (Controllability)

信息可控性是指能够控制使用信息资源的人或主体的使用方式。对于信息系统中的敏感信息资源,如果任何主体都能访问、篡改、窃取和恶意散播的话,安全系统显然会失去了效用。对访问信息资源的人或主体的使用方式进行有效控制,是信息安全的必然要求,从国家层面看,信息安全的可控性不但涉及信息的可控性,还与安全产品、安全市场、安全厂商、安全研发人员的可控性紧密相关。信息的可控性主要通过基于公钥基础设施(PKI, Public Key Infrastructure)/授权管理基础设施(PMI, Privilege Management Infrastructure)的访问控制技术来保证。

可控性应该满足以下要求:身份识别与验证、访问控制(对用户的权限进行控制,只能访问相应权限的资源,防止或限制经隐蔽通道的非法访问,包括自主访问控制和强制访问控制)、业务流控制(利用均分负荷方法,防止业务流量过度集中而引起网络阻塞)、路由选择控制(选择那些稳定可靠的子网、中继线或链路等)、审计跟踪(审计跟踪的信息主要包括事件类型、被管客体等级、事件时间、事件信息、事件回答和事件统计等方面的信息)。

从控制的对象来说,可控性可以分为以下几个方面。

(1) 实体可信。保证构建网络的基础设备和软件系统安全可信,没有预留后门或逻辑炸弹。保证接入网络的用户是可信的,防止恶意用户对系统的攻击破坏;保证在网络上传输、处理、存储的数据是可信的,防止搭线窃听、非授权访问或恶意篡改。

(2) 行为可控。保证本地计算机的各种软硬件资源(如内存、中断、I/O 端口、硬盘等硬件设备,文件、目录、进程、系统调用等软件资源)不被非授权使用或不被用于危害本系统或其他系统的安全;保证网络接入可控,即保证用户接入网络应严格受控,用户上网必须申请登记并得到许可;保证网络行为可控,即保证网络上的通信行为受到监视和控制,防止滥用资源、非法外联、网络攻击、非法访问和传播有害信息等恶意事件的发生。

(3) 资源可管。保证对路由器、交换机、服务器、邮件系统、目录系统、数据库、域名系统、安全设备、密码设备、密钥参数、交换机端口、IP 地址、用户账号、服务端口等

网络资源进行统一管理。

(4) 事件可查。保证对网络上的各类违规事件进行监控记录，确保日志记录的完整性，为安全事件稽查、取证提供依据。

(5) 运行可靠。保持对网络信息运行的可用性的控制，即保证网络节点在发生自然灾害或遭到硬摧毁时仍能不间断运行，具有容灾抗毁和备份恢复能力；保证能够有效防范病毒和黑客的攻击所引起的网络拥塞、系统崩溃和数据丢失，并具有较强的应急响应和灾难恢复能力。

## 2. 安全防御的机制

网络信息安全防御的机制如图 7-2 所示。



图 7-2 安全防御机制

(1) 加密 (Encipherment)，隐藏或覆盖信息以使其具有机密性；还可以用来执行提供别的服务的其他机制。今天，有加密术和密写术两种技术被用来加密。

(2) 信息的完整性 (Information integrity)，该机制附加于一个短的键值，该键值是信息本身创建的特殊程序。接收方接收信息和键值，再从接收的信息中创建一个新的键值，并把新创建的键值和原来的进行比较。如果两个键值相同，则说明信息的完整性被保全。

(3) 数字签名 (digital signature)，通过这种方法信息发送方可以对信息进行电子签名，信息接收方可以对签名进行电子检验。发送方使用显示其与公钥有联系的私钥，这个公钥是他公开承认的。接收方使用发送方的公钥，证明信息确实是由声称发送过这个信息的人签名的。

(4) 身份认证交换 (authentication exchange)，进行身份认证交换时，两个实体交换信息以相互证明身份。例如，一方实体可以证明他知道一个只有他才知道的秘密。

(5) 流量填充 (traffic padding)，是指在数据流中嵌入一些虚假信息，从而阻止对手企图使用流量分析。

(6) 路由控制 (routing control)，是指在发送方和接收方之间选择并不断改变有效路由，以避免对手在特定的路由上进行偷听。

(7) 公证 (notarization)，是指选择一个双方都依赖的第三方控制双方的通信，如此即可避免否认。为了避免发送方过后否认其曾经提过这样的请求，接收方可以牵涉第三方来保存发送方的请求。

(8) 访问控制 (access control)，就是用各种方法，证明某用户具有访问该信息或系统所拥有的资源的权利。如密码和个人标识号 (PIN, Personal Identification Number)，就是这方面的例子。

3. 安全防御属性和机制之间的关系

安全防御属性和机制的关系见表 7-1。此表表明三种机制（加密、数字签名和身份认证交换）均可被用来提供身份认证，也表明加密机制在三种服务（信息机密性、信息完整性和身份认证）中都会被涉及。

表 7-1 安全防御属性和机制的关系

安全防御属性	安全防御机制
机密性	加密和路由控制
完整性	加密、数字签名、信息完整性
可用性	加密、数字签名、身份认证交换、信息完整性
不可否认性	数字签名、信息完整性和公证
可控制	访问控制

7.1.4 网络信息安全等级保护的法律法规和政策标准

信息安全等级保护是指对国家秘密信息、法人和其他组织及公民的专有信息，以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应、处置。

1. 等级的划分

根据安全保护能力，网络信息安全被划分为五个等级：第一级为用户自主保护级；第二级为系统审计保护级；第三级为安全标记保护级，第四级为结构化保护级；第五级为访问验证保护级。根据主体遭受破坏后对客体的破坏程度而设立的监管强度等级共分五级：第一级为自主保护级；第二级为指导保护级；第三级为监督保护级；第四级为强制保护级；第五级为专控保护级。

按照两种等级划分描述的对对应关系见表 7-2。

表 7-2 信息系统安全等级划分对应表

等 级	监 管 强 度	保 护 能 力	侵害客体及侵害程度
第一级	自主保护级	用户自主保护级	信息系统受到破坏后，会对公民、法人和其他组织的权益有一定影响，但不危害国家安全、社会秩序、经济建设和公共利益
第二级	指导保护级	系统审计保护级	信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，不影响国家安全
第三级	监督保护级	安全标记保护级	信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害
第四级	强制保护级	结构化保护级	信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害
第五级	专控保护级	访问验证保护级	信息系统受到破坏后，会对国家安全造成特别严重的损害

## 2. 我国相关的法律、法规和政策文件

### 1) 相关法律

信息安全法律是由国家立法机关“全国人民代表大会及其常务委员会”，按照严格的立法程序，对信息安全方面的重大问题制定和颁布的法律和法令等。涉及的法律有以下几项：

(1) 1988年9月5日，第七届全国人民代表大会常务委员会第三次会议通过的《中华人民共和国保守国家秘密法》。

(2) 1995年2月28日，全国人民代表大会第12次会议通过并实施的《中华人民共和国警察法》第二章第六条第十二款规定，公安机关警察依法履行“监督管理计算机信息系统的安全保护工作”。

(3) 2016年11月7日，第十二届全国人民代表大会常务委员会第二十四次会议通过了《中华人民共和国网络安全法》。

### 2) 相关法规

信息安全保护的法规是国家、军队和地方颁布的一切信息安全防护的法律规范、条令、条例、规定、规则、标准、章程及制度的总称。相关的法规较多，主要有以下一些。

(1) 1989年，公安部发布了《计算机病毒控制规定（草案）》。

(2) 1993年10月26日，中央军委颁布了《中国人民解放军技术安全保密条例》。共9章38条，包括总则、涉密技术系统安全保密、涉密信息和数据安全保密、涉密场所安全保密、计算机病毒防治、技术安全保密防护产品管理、监督检查、奖励处罚、附则等内容。

(3) 1994年2月18日，国务院发布《中华人民共和国计算机信息系统安全保护条例》（国务院147号令）；2011年1月8日进行了修订。

(4) 1994年6月4日，国务院发布了《中华人民共和国国家安全法实施细则》。1996年2月1日，国务院发布《中华人民共和国计算机信息网络国际联网管理暂行规定》。

(5) 1996年3月24日，中央军委颁布了《中国人民解放军保密条例》，此案例是用于规范军队保密工作的一部专门法规，为全军各单位制定保密规章和制度提供了基本依据。

(6) 1999年9月13日，公安部组织有关单位和专家起草了安全保护等级管理的重要基础性国家强制性标准——《计算机信息系统安全保护等级划分准则》正式批准发布。

(7) 2000年11月，国务院新闻办公室和信息产业部（现为工业和信息化部）联合发布《互联网站从事登载新闻业务管理暂行规定》。

(8) 2000年11月，信息产业部（现为工业和信息化部）发布《互联网电子公告服务管理规定》。

(9) 2000年12月28日，为规范互联网用户的行为，第九届全国人民代表大会常委会通过了《全国人大常委会关于维护互联网安全的决定》。

(10) 2001年2月，经中央军委批准，解放军四总部联合签署了《中国人民解放军计

算机信息系统安全保密规定》((2001)参字第1号)。

(11) 2001年12月20日,国务院令第339号公布《计算机软件保护条例》;2013年1月30日第二次修订。

(12) 2006年5月18日,国务院令第468号公布《信息网络传播权保护条例》;2013年1月30日修订。

(13) 2008年6月10日,公安部发布了《公安机关信息安全等级保护检查工作规范(试行)》(公信安〔2008〕736号),这是指导监督检查环节工作的法规文件。

(14) 2013年7月16日,工业和信息化部第24号令公布《电信和互联网用户个人信息保护规定》,自2013年9月1日起施行。

### 3) 政策文件

(1) 1996年1月23日,国务院第42次常务会议通过并发布了《中华人民共和国计算机信息网络国际联网管理暂行规定实施办法》,1997年5月20日修订。

(2) 1997年5月,国务院信息化工作领导小组发布《中国互联网络域名注册暂行管理办法》。

(3) 1997年,原邮电部发布《国际互联网出入信道管理办法》。

(4) 1997年12月11日,国务院批准《计算机信息网络国际联网安全保护管理办法》(公安部令第33号)。2011年1月8日修订。

(5) 2000年9月25日,国务院令第292号公布《互联网信息服务管理办法》。2011年1月8日修订。

(6) 2003年,中央办公厅、国务院办公厅转发的《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发〔2003〕27号)明确指出:要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统,抓紧建立信息安全等级保护制度。制定信息安全等级保护的管理办法和技术指南。

(7) 2004年,公安部、国家保密局、国家密码管理局、国家信息化工作办公室出台了《关于信息安全等级保护工作的实施意见》(66号文件)。

(8) 2005年7月1日,国家保密局公布的《涉及国家秘密的计算机信息系统集成资质管理办法》开始施行。

(9) 2006年1月,公安部、国家保密局、国家密码管理局、国家信息化工作办公室联合出台《信息安全等级保护管理办法(试行)》。

(10) 2007年6月22日,公安部、国家保密局、国家密码管理局、国家信息化工作办公室联合出台《信息安全等级保护管理办法》(公通字〔2007〕43号)。

(11) 2007年7月16日,公安部、国家保密局、国家密码管理局和国务院信息化工作办公室联合发布《关于开展全国重要信息系统安全等级保护定级工作的通知》(公信安〔2007〕861号)。这是一部指导定级环节工作的政策文件。

(12) 2008年8月6日,国家发展和改革委员会、公安部、国家保密局共同发布了《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》(发改高技〔2008〕2071

- 号), 明确了项目验收条件, 目的是加强基础信息网络和重要信息系统安全保障。
- (13) 2009 年 10 月 27 日, 公安部发布了《关于开展信息系统等级保护安全建设整改工作的指导意见》公信安〔2009〕1429 号, 明确了非涉及国家秘密信息系统开展安全建设整改工作的目标、内容、流程和要求等。
- (14) 2009 年 11 月 6 日, 公安部十一局发布了《关于印发〈信息系统安全等级测评报告模板(试行)〉的通知》公信安〔2009〕1487 号, 明确了等级测评活动的内容、方法和测评报告格式等。
- (15) 2010 年 10 月 27 日, 公安部发布了《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》(公信安〔2010〕303 号), 确定了开展信息安全等级保护测评体系建设和等级测评工作的目标、内容和工作要求。
- (16) 2014 年 5 月 9 日, 中央网络安全和信息化领导小组办公室发布了《关于加强党政机关网站安全管理的通知》(中网办〔2014〕1 号)。
- (17) 2016 年 8 月 12 日, 中央网络安全和信息化领导小组办公室、国家质量监督检验检疫总局和国家标准化管理委员会联合发布《关于加强国家网络安全标准化工作的若干意见》。
- (18) 2016 年 12 月 27 日, 国家互联网信息办公室发布《国家网络空间安全战略》报告。
- (19) 2017 年 3 月 1 日, 中国外交部和国家互联网信息办公室共同发布了《网络空间国际合作战略》, 战略确立了中国参与网络空间国际合作的六大战略目标。

3. 标准体系

为推动我国信息安全等级保护工作, 全国信息安全标准化技术委员会和公安部信息系统安全标准化技术委员会组织制定了信息安全等级保护工作需要的一系列标准, 为开展等级保护工作提供了标准保障。这些标准可以分为基础类、应用类、产品类和其他类, 已经发布和提交报批的标准分类统计见表 7-3。

表 7-3 信息系统安全等级保护相关标准列表

标准类型	子 类 型	标 准 名 称
基础类		计算机信息系统安全保护等级划分准则 (GB 17859—1999)
应用类	信息系统定级	信息系统安全保护等级定级指南 (GB/T 22240—2008)
	等级保护实施	信息系统安全等级保护实施指南 (信安字〔2007〕10 号)
	信息系统安全建设	信息系统安全等级保护基本要求 (GB/T 22239—2008)
		信息系统安全管理要求 (GB/T 20269—2006)
		网络基础安全技术要求 (GB/T 20270—2006)
		信息系统通用安全技术要求 (GB/T 20271—2006)
		信息系统安全工程管理要求 (GB/T 20282—2006)
		信息系统物理安全技术要求 (GB/T 21052—2007)
		信息系统安全等级保护体系框架 (GA/T 708—2007)
		信息系统安全等级保护基本模型 (GA/T 709—2007)
		信息系统安全等级保护基本配置 (GA/T 710—2007)
		信息系统等级保护安全设计技术要求 (GB/T 24856—2009)



续表

标准类型	子 类 型	标 准 名 称
应用类	安全测评	信息系统安全管理测评 (GA/T 713—2007)
		信息系统安全等级保护测评要求
		信息系统安全等级测评过程指南
产品类	操作系统	操作系统安全评估准则 (GB/T 20008—2005)
		操作系统安全技术要求 (GB/T 20272—2006)
	数据库	数据库管理系统安全评估准则 (GB/T 20009—2005)
		数据库管理系统安全技术要求 (GB/T 20273—2006)
	网络设备	网络端设备隔离部件技术要求 (GB/T 20279—2006)
		网络端设备隔离部件测试评价方法 (GB/T 20277—2006)
		网络脆弱性扫描产品技术要求 (GB/T 20278—2006)
		网络脆弱性扫描产品测试评价方法 (GB/T 20280—2006)
	交换机	网络交换机安全技术要求 (GA/T 684—2007)
		交换机安全测评要求 (GA/T 685—2007)
		网络交换机安全技术要求 (GB/T 21050—2007)
	路由器	路由器安全评估准则 (GB/T 20011—2005)
		路由器安全技术要求 (GB/T 18018—2007)
		路由器安全测评要求 (GA/T 682—2007)
	网关	网关安全技术要求 (GA/T 681—2007)
	虚拟专用网 (VPN)	虚拟专用网安全技术要求 (GA/T 686—2007)
	防火墙	包过滤防火墙评估准则 (GB/T 20010—2005)
		防火墙技术要求和测评方法 (GB/T 20281—2006)
		防火墙安全技术要求 (GA/T 683—2007)
		防火墙技术测评方法
		信息系统安全等级保护防火墙安全配置指南
	入侵检测 (IDS)	入侵检测系统技术要求和检测方法 (GB/T 20275—2006)
		计算机网络入侵分级要求 (GA/T 700—2007)
	PKI	公钥基础设施安全技术要求 (GA/T 687—2007)
		PKI 系统安全等级保护技术要求 (GB/T 21053—2007)
	审计产品	审计产品技术要求和测评方法 (GB/T 20945—2006)
	身份认证	虹膜特征识别技术要求 (GB/T 20979—2007)
	服务器	服务器安全技术要求 (GB/T 21028—2007)
	终端计算机	终端计算机系统安全等级技术要求 (GA/T 671—2006)
		终端计算机系统测评方法 (GA/T 672—2006)
	应用软件系统	应用软件系统安全等级保护通用技术指南 (GA/T 711—2007)
		应用软件系统安全等级保护通用测试指南 (GA/T 712—2007)
	风险评估	信息安全风险评估规范 (GB/T 20984—2007)
其他类	安全事件	信息安全事件管理指南 (GB/T 20985—2007)
		信息安全事件分类分级指南 (GB/T 2986—2007)
		信息系统灾难恢复规范 (GB/T 20988—2007)

### 7.1.5 网络空间信息防御体系的层次结构

一个全方位的网络空间信息防御体系层次结构包括法律规范、安全管理、物理安全、网络安全、系统安全、应用安全和信息安全。这就是所谓的信息安全纵深防御层次体系。可以用图 7-3 表示它们的逻辑层次结构分布。

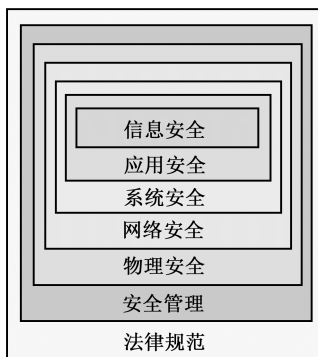


图 7-3 网络空间信息防御体系逻辑层次结构分布图

从图 7-3 中可知，信息安全是目标，其余可成为安全保护的过程。要保障信息的安全性，必须有安全可靠的应用系统，如 WWW 服务、E-mail 邮件服务、电子政务、PKI 等；要保障以上应用系统安全首先要有安全可靠的计算机系统作保障，包括计算机硬件、软件、数据库、操作系统等；其次必须有安全可靠的网络环境，包括身份认证、访问控制、防病毒、防黑客入侵、数据传输的加密与解密等；物理安全是以上安全保障的基础，如果机器被盗、水淹、火烧等以上工作都是徒劳；有再好的技术，没有好的安全管理策略和安全管理制度安全保护就成为一句空话；最后要以法律规范为依据，约束个人行为，提高每个人的安全意识，共同建造信息安全的大环境，促进信息化高速发展。

#### 1. 法律规范

要进一步加强依法治网、依法办网、依法上网，用法治规范网络空间的行为。国外互联网企业进入中国，底线是遵守中国的法律法规，不得损害中国国家利益和中国公民的合法权益。所以要加大政策的研究与制定，建立一系列规章制度、法律法规和标准规范，为网络空间防御体系建设提供有效的支撑。

#### 2. 安全管理

安全管理的内容包括人员及其培训管理、软件及应用系统管理、安全技术和设备管理、文档和数据管理、操作及其运行管理、机房管理、工作日志管理、应急管理、安全职责划分、人员角色配置等。通过管理安全措施，为安全防范体系各个方面建立安全策略，形成安全制度，并保障各项管理制度落到实处。

3. 物理安全（也称实体安全）

物理安全，就是保证计算机信息系统各种设备的安全，是整个计算机信息系统安全的前提。物理安全的主要内容见表 7-4。

表 7-4 物理安全

物 理 安 全		
环 境 安 全	设 备 安 全	媒 体 安 全
环境保护、区域保护、灾难保护、机房保护、建筑保护、运行环境（温度、湿度、烟尘）、影响因素	防盗、防电磁泄漏、防线路截获、辐射控制、抗干扰、软硬件保护、设备备份、动力与电源保护、灾难预防与恢复	通信线路安全、媒体本身的安全、数据的安全、数据的处理

4. 网络安全

计算机网络是应用数据的传输通道，并控制流入、流出内部网的信息流。它包括网络层身份认证，网络资源的访问控制，数据传输的保密与完整性，远程接入的安全，域名系统的安全，路由系统的安全，入侵检测的手段，网络设施防病毒等。网络安全最主要的任务是规范其连接方式，加强访问控制，部署安全保护产品，建立相应的管理制度并贯彻实施。网络安全的主要内容见表 7-5。

表 7-5 网络安全

网 络 安 全			
访 问 控 制	身 份 验 证	运 行 安 全	内 网 安 全
防火墙、物理隔离	传统身份验证（标志、口令）、数字鉴别、Kerberos	系统备份、数据容灾、备份与恢复、网络防毒	虚拟局域网、入侵检测、非法外联监控

5. 系统安全

系统（平台）安全主要保护主机上的操作系统与数据库系统的安全。操作系统的安全包括安全操作系统的模型和实现、操作系统的安全加固、操作系统的脆弱性分析、操作系统与其他开发平台的安全关系等。数据库系统安全是指为数据库系统采取的安全保护措施，防止系统软件和其中数据遭到破坏、更改和泄露。目前操作系统与数据库系统都是非常成熟的产品，安全功能较为完善。对于保证系统（平台）安全，总体思路是先通过安全加固解决企业管理方面存在的安全漏洞，然后采用安全技术设备来增强其安全防护能力。系统安全的主要内容见表 7-6。

表 7-6 系统安全

系 统 安 全		
安 全 漏 洞	操 作 系 统	数据库系统安全
漏洞分类、漏洞扫描	安全配置、安全策略	数据库安全框架、数据加密、主机加固

## 6. 应用安全

应用安全是保护应用系统的安全、稳定运行，保障用户的合法权益。它包括业务软件的安全性测试，业务交往的防抵赖性测试，业务资源的访问控制验证测试，业务实体的身份鉴别检测，业务现场的备份与恢复机制检查，业务数据的唯一性、一致性、防冲突检测 and 保密性测试，业务系统的可靠性和可用性测试等。应用安全的主要内容见表 7-7。

表 7-7 应用安全

应用安全			
Web 安全	E-mail 安全	电子政务	公钥基础设施 (PKI)
Web 服务、安全措施	邮件加密、邮件信息过滤	纵深防御、安全策略	PKI 服务、标准、体系

## 7. 信息安全

信息安全是指防止信息资源的非授权泄露、更改、破坏，或使信息被非法系统辨识、控制和否认。也就是：确保信息的完整性、机密性、可用性和可控性；保护网络中的数据不被篡改、非法增删、复制、解密、显示、使用等；防止信息丢失、崩溃和被非法访问；介质与载体的安全保护；信息检查、标志、鉴别、监控和审计；信息存储与备份安全；等等。

### 7.1.6 网络空间信息防御的体系结构

网络空间信息防御体系能力是网络空间信息防御体系实施网络防御作战时所具备或发挥的能力。它是以网络技术和信息技术为支撑和纽带，将网络空间信息防御体系内各组成系统相互融合，集成为一体，密切协同，形成的具有倍增效应的体系化作战能力。

网络空间信息防御体系由指挥管理系统、网络侦察系统、网络预警系统、网络防护系统、入侵检测系统、应急响应系统、网络恢复系统、威慑反击系统、应用保障系统等 9 大系统组成。这 9 大系统按网络空间信息防御作战进程展开，实时联动，在网络空间信息防御统一策略指导下，融合成一个有机整体。网络空间信息防御体系的详细结构如图 7-4 所示。

指挥管理系统是网络空间信息防御体系的“大脑”，负责制定网络空间信息防御决心、拟制防御计划、组织管理防御进程、指挥协调防御行动并实时评估防御作战效果；网络侦察系统是网络空间信息防御体系的“耳目”，通过不间断地侦察网络空间的敌情变化，搜集和整理敌方网络攻击情报；网络预警系统是网络空间信息防御体系的“哨兵”，通过实时侦测，识别威胁，评估态势，及时发出预警信息，化被动防御为主动防御；网络防护系统是网络空间信息防御体系的“长城”，通过采取伪装、密码、控制、隔离、扫描等有效措施不断提高体系的安全防护系数，筑牢防护屏障；入侵检测系统是网络空间信息防御体系的“电子眼”，检测穿过网络防护系统进入体系内部的入侵信息、发现入侵行为，拦截网络攻击；应急响应系统是网络空间信息防御体系的“急救车”，对网络空间信息入侵做

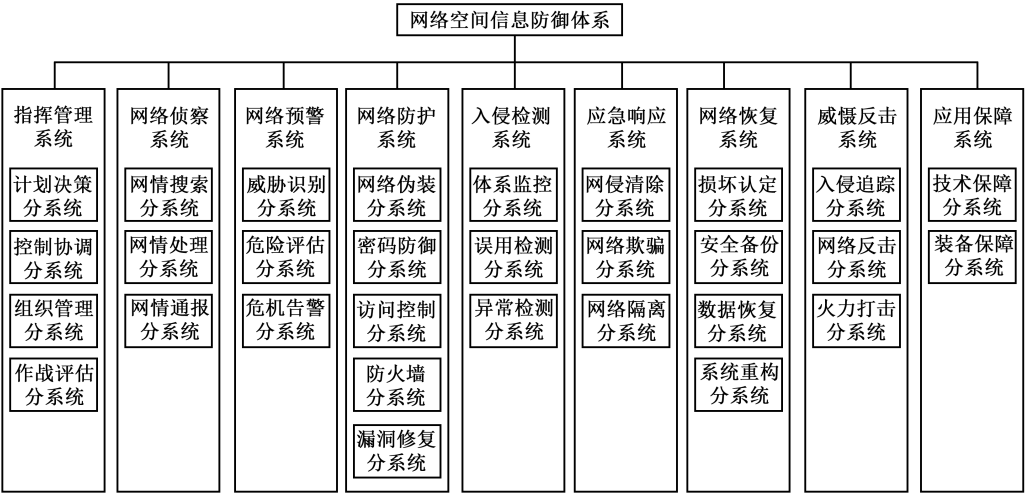


图 7-4 网络空间信息防御体系结构

出及时回应，阻止、清除各类入侵；网络恢复系统是网络空间信息防御体系的“自救系统”，对遭受攻击破坏的系统和数据根据备份信息进行数据恢复和系统重构，提高体系抗毁性；威慑反击系统是网络空间信息防御体系的“铁拳”，应用网络攻击和实体打击手段对网络空间信息入侵之敌进行报复性反击，慑止其进一步攻击企图；应用保障系统是网络空间信息防御体系的“基石”，为网络空间信息防御体系提供所需的各类技术和装备保障支持。

图 7-5 是基于美国国防部信息系统安全计划（DISSP）扩展的一个三维安全防范技术体系框架结构。第一维是安全服务，给出了八种安全属性（ITU-TREC-X.800-199103-1）。第二维是系统单元，给出了信息网络系统的组成。第三维是结构层次，给出并扩展了国际标准化组织（ISO，International Organization for Standardization）的开放系统互联参考模型（OSI，Open System Interconnect Reference Model）。

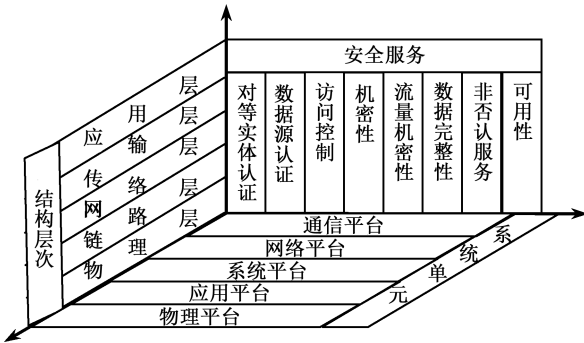


图 7-5 三维安全防范技术体系框架结构

框架结构中的每一个系统单元都对应于某一个协议层次，需要采取若干种安全服务才能保证该系统单元的安全。网络平台需要有网络节点之间的认证、访问控制；应用平台需

要有针对用户的认证、访问控制，需要保证数据传输的完整性、保密性，需要有抗抵赖和审计的功能，需要保证应用系统的可用性和可靠性。针对一个信息网络系统，如果在各个系统单元都有相应的安全措施来满足其安全需求，那么我们认为该信息网络是安全的。

### 7.1.7 网络空间安全防护过程

网络空间安全防护是一个动态过程，只有不断地做出相应变化调整，才能保证安全防护系统的有效性。

(1) 进行态势分析。预测和评估当前和预计的网络安全威胁产生的致命性后果带来的影响和损失，对网络的安全态势有一个清晰、客观和全面的了解。

(2) 确立安全防护目标。针对要实现的安全（防御和威胁）程度以及实现的日期做出定量和定性的详细表述。

(3) 选择安全防护策略。基于安全漏洞的普遍性和威胁的不确定性，制定满足安全目标的可供选择方法。

(4) 制定安全防护计划。对各种可供选择的防御方法加以分析评估，根据其效能、可行性、风险等指标进行决策，将计划要素（风险分析、保护、指示和预警、响应、灾难恢复）综合成一个一致的安全计划。

(5) 及时风险评估。为贯彻防御计划，制定一个度量和控制风险的方法，对风险发生的概率以及结果进行量化。针对每个风险领域制定其消除防范计划。

(6) 实施实时监控。对所贯彻行动的效果和性能进行过程监控，并可根据出现的偏差进行改进调整。

网络空间安全防护作战主要包括四个组成部分：预防、指示与告警、检测和响应，是一个闭环反馈过程，是简单的叠加、融合和交互，其运行过程具体描述如图 7-6 所示。同时，网络空间安全防护的运行过程具有系统性、闭环性和联合性的特性。

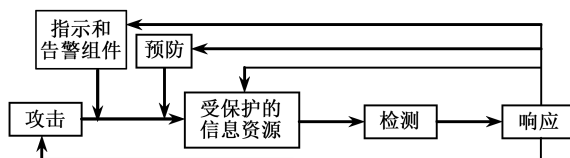


图 7-6 网络空间安全防护的运行过程

(1) 系统性。网络安全防御是个综合性的课题，木桶原理形象地说明了这一点。网络防御体系必须具有系统性的特征，多种安全技术要实现相互间的协作和融合，这样的协作与融合将会是防御能力的倍增器。

(2) 闭环性。防御体系是否可行，关键一点就在于体系是否为闭环，即能否自动适应网络攻击行为的变化和新型攻击的出现。这种适应或反馈也必须通过技术手段自动完成。

(3) 联合性。整个网络的防御体系是上面基本体系的叠加、融合和交互。联合就是对某一基本单元的攻击事件能及时传递到其他基本单元, 便于做好防御和应对工作。

### 7.1.8 网络安全防范体系设计准则

根据防范攻击的安全需求、需要达到的安全目标、对应安全机制所需的安全服务等因素, 参照 SSE-CMM (系统安全工程能力成熟模型) 和 ISO 17799 (信息安全管理标准) 等国际标准, 综合考虑可实施性、可管理性、可扩展性、综合完备性和系统均衡性等方面, 网络安全防范体系在整体设计过程中应遵循 9 项原则, 下面分别进行介绍。

#### 1) 网络信息安全的木桶原则

木桶原则是指对信息进行均衡、全面的保护。“木桶的最大容积取决于最短的一块木板”。网络信息系统是一个复杂的计算机系统, 它本身在物理上、操作上和管理上的种种漏洞构成了系统的安全脆弱性, 尤其是多用户网络系统自身的复杂性、资源共享性使单纯的技术保护防不胜防。攻击者使用的“最易渗透原则”, 必然在系统中最薄弱的地方进行攻击。因此, 充分、全面、完整地对系统的安全漏洞和安全威胁进行分析、评估和检测 (包括模拟攻击) 是设计信息安全系统的必要前提条件。网络安全防御设计的首要目的是防止最常用的攻击手段, 根本目的是提高整个系统的“安全最低点”的安全性能。

#### 2) 网络信息安全的整体性原则

整体性原则要求在网络发生被攻击、破坏事件的情况下, 必须尽可能地快速恢复网络信息中心的服务, 减少损失。因此, 信息安全系统应包括安全防护机制、安全检测机制和安全恢复机制。安全防护机制是根据具体系统存在的各种安全威胁而采取的相应的防护措施, 避免非法攻击的进行。安全检测机制是检测系统的运行情况, 及时发现和制止对系统进行的各种攻击。安全恢复机制是在安全防护机制失效情况下, 进行应急处理和尽量、及时地恢复信息, 减少供给的破坏程度。

#### 3) 安全性评价与平衡原则

对任何网络, 绝对安全难以达到, 也不一定是必要的, 所以需要建立合理的实用安全性与用户需求评价与平衡体系。安全防御体系设计要正确处理需求、风险与代价的关系, 做到安全性与可用性相兼顾, 做到组织上可执行。评价信息是否安全, 没有绝对的评判标准和衡量指标, 只能决定于系统的用户需求和具体的应用环境, 具体取决于系统的规模、范围、性质和信息的重要程度。

#### 4) 标准化与一致性原则

系统是一个庞大的系统工程, 其安全体系的设计必须遵循一系列的标准, 这样才能确保各个分系统的一致性, 使整个系统安全地互联互通、信息共享。

### 5) 技术与管理相结合原则

安全体系是一个复杂的系统工程，涉及人、技术、操作等要素，单靠技术或单靠管理都不可能实现。因此，必须将各种安全技术与运行管理机制、人员思想教育与技术培训、安全规章制度建设相结合。

### 6) 统筹规划，分步实施原则

由于政策规定、服务需求的不明朗，环境、条件、时间的变化，攻击手段的进步，安全防护不可能一步到位，可在一个比较全面的安全规划下，根据网络的实际需要，先建立基本的安全体系，保证基本的、必需的安全性。今后随着网络规模的扩大及应用的增加，网络应用和复杂程度的变化，网络脆弱性也会不断增加，调整或增强安全防护力度，才能保证整个网络最根本的安全需求。

### 7) 等级性原则

等级性原则是指安全层次和安全级别。良好的信息安全系统必然是分为不同等级的，包括对信息保密程度分级，对用户操作权限分级，对网络安全程度分级（安全子网和安全区域），对系统实现结构的分级（应用层、网络层、链路层等），从而针对不同级别的安全对象，提供全面、可选的安全算法和安全体制，以满足网络中不同层次的各种实际需求。

### 8) 动态发展原则

根据网络安全的变化不断调整安全措施，适应新的网络环境，满足新的网络安全需求。

### 9) 易操作性原则

首先，安全措施需要人去完成，如果措施过于复杂，对人的要求过高，本身就降低了安全性。其次，措施的采用不能影响系统的正常运行。

## 7.2 网络空间作战的预防手段

网络空间预防技术是网络防御中最基础、最常用的手段，也是网络防御的第一道屏障，目前主要的预防手段有防火墙技术、防病毒技术、数据加密技术、信息隐藏技术、访问控制技术。下面就从这 5 种技术手段进行详细的介绍。

### 7.2.1 防火墙技术

所谓防火墙，指的是一个由软件和硬件设备组合而成，在内部网和外部网之间、专用



网与公网之间的界面上构造的保护屏障，是两网之间信息的唯一出入口。它通过在网络边界上建立相应的安全控制点、网络通信监控系统或安全控制策略（允许、拒绝、监测）来隔离保护网络和外部网络，对进出网络的数据报文进行分析、检测和过滤，从而达到限制非法流量的流入。在逻辑上，防火墙是一个分离器，一个限制器，也是一个分析器，允许“同意”的人和数据进入保护网络，同时将“不同意”的人和数据拒之门外。

防火墙的好处是能有效监控两网之间的任何活动，集中进行安全管理，防止外部网络用户未经授权的访问，防止内部信息的外泄，对进、出保护网络（主机）的存取、服务和访问进行监控审计，记录和统计非法使用数据情况，阻挡来自外部的网络入侵，保护脆弱的服务，增强保密性，从而保证保护网络的安全。

### 1. 防火墙的分类

从技术角度来看，目前有两类防火墙，即标准防火墙和双穴网关。标准防火墙使用专门的软件，并要求比较高的管理水平，而且在信息传输上有一定的延迟。双穴网关是标准防火墙的扩充，也称应用层网关，它是一个独立的系统，但能够同时完成标准防火墙的所有功能。它的优点是能够运行比较复杂的应用，同时防止在互联网和内部系统之间建立任何直接连接，可以确保数据包不能直接从外部网络到达内部网络。

从实现原理上分，防火墙的技术包括五大类：网络级防火墙（也叫包过滤型防火墙）、应用级网关、电路级网关、规则检查防火墙和状态监测防火墙。它们之间各有所长，具体使用哪一种或是否混合使用，要看具体需要。

（1）网络级防火墙。一般是基于源地址和目的地址、应用、协议以及每个 IP 包的端口来作出通过与否的判断。一个路由器便是一个传统的网络级防火墙，大多数的路由器都能通过检查这些信息来决定是否将所收到的包转发，但它不能判断出一个 IP 包来自何方，去向何处。网络级防火墙会按照系统管理员所给定的过滤规则进行过滤，如果对防火墙设定某一 IP 地址的站点为不适宜访问，那么从这个地址来的所有信息都会被防火墙屏蔽掉。

（2）应用级网关。应用级网关能够检查进出的数据包，通过网关复制传递数据，防止在受信任服务器和客户机与不受信任的主机间直接建立联系。应用级网关能够理解应用层上的协议，能够做复杂一些的访问控制，并做精细的注册和稽核。它针对特别的网络应用服务协议即数据过滤协议，并且能够对数据包分析并形成相关的报告。应用级网关有较好的访问控制，是目前最安全的防火墙技术，但实现困难，而且有的应用级网关缺乏透明度。

（3）电路级网关。用来监控受信任的客户或服务器与不受信任的主机间的 TCP 握手信息，这样来决定该会话是否合法。电路级网关是在 OSI 模型中会话层上来过滤数据包，这样比包过滤防火墙要高两层。电路级网关还提供一个重要的安全功能：代理服务器（Proxy Server）。代理服务器是个防火墙，是设置在因特网防火墙网关的专用应用级代码，在其上运行一个叫作“地址转移”的进程，来将所有内部的 IP 地址映射到一个安全的 IP 地址，这个地址是由防火墙使用的。

（4）规则检查防火墙。该防火墙结合了包过滤防火墙、电路级网关和应用级网关的特点。它同包过滤防火墙一样，规则检查防火墙能够在 OSI 网络层上通过 IP 地址和端口号，过滤进出的数据包。它也像电路级网关一样，能够检查 SYN 和 ACK 标记和序列数字是否

逻辑有序。当然它也像应用级网关一样，可以在 OSI 应用层上检查数据包的内容，查看这些内容是否能符合网络的安全规则。规则检查防火墙虽然集成前三者的特点，但是不同于一个应用级网关防火墙的是，它并不打破客户机/服务器模式来分析应用层的数据，它允许受信任的客户机和不受信任的主机建立直接连接。规则检查防火墙不依靠与应用层有关的代理，而是依靠某种算法来识别进出的应用层数据，这些算法通过已知合法数据包的模式来比较进出数据包，这样从理论上就能比应用级代理在过滤数据包上更有效。

(5) 状态监测防火墙。使用了一个在网路上执行网络安全策略的软件模块，称之为监测引擎。监测引擎在不影响网络正常运行的前提下，采用抽取有关数据的方法对网络通信的各层实施监测，抽取状态信息，并动态地保存起来作为以后执行安全策略的参考。监测引擎支持多种协议和应用程序，并可以很容易地实现应用和服务的扩充。当用户访问请求到达网关的操作系统前，状态监视器要抽取有关数据进行分析，结合网络配置和安全规定做出接纳、拒绝、身份认证、报警或给该通信加密等处理动作。一旦某个访问违反安全规定，就会拒绝该访问，并报告有关状态做日志记录。状态监测防火墙的另一个优点是它会监测无连接状态的 RPC 和 UDP 之类的端口信息。这种防火墙无疑是非常坚固的，但会降低网络速度，而且配置也比较复杂。

## 2. 主要技术

先进的防火墙产品将网关与安全系统合二为一，具有以下技术与功能。

(1) 结构。新一代防火墙产品具有两个或三个独立的网卡。若是三个独立的网卡。内外两个网卡可不作 IP 转化而串接于内部网与外部网之间，另一个网卡可专用于对服务器的安全保护。

(2) 访问方式。以前的防火墙在访问方式上要么要求用户进行系统登录，要么需要通过防火墙安全会话转换协议 (SOCKS, Protocol for Sessions Traversal Across Firewall Securely) 等路径修改客户机的应用。新一代防火墙利用了透明的代理系统技术，从而降低了系统登录固有的安全风险和出错概率。

(3) 代理系统。代理系统是一种将信息从防火墙的一侧传送到另一侧的软件模块。新一代防火墙采用了两种代理机制，一种用于代理从内部网络到外部网络的连接，另一种用于代理从外部网络到内部网络的连接。前者采用网络地址转换 (NAT, Network Address Translation) 技术来解决，后者采用非保密的用户定制代理或保密的代理系统来解决。

(4) 过滤技术。为保证系统的安全性和防护水平，新一代防火墙采用了三级过滤措施，并辅以鉴别手段。在分组过滤一级，能过滤掉所有的源路由分组和假冒的 IP 源地址；在应用级网关一级，能利用 FTP、简单邮件传输协议 (SMTP, Simple Mail Transfer Protocol) 等各种网关，控制和监测因特网提供的所用通用服务；在电路网关一级，实现内部主机与外部站点的透明连接，并对服务的通行实行严格控制。

(5) 转换技术。新一代防火墙利用 NAT 技术能透明地对所有内部地址进行转换，使外部网络无法了解内部网络的内部结构，同时允许内部网络使用自己定制的 IP 地址和专用网络，防火墙能详尽记录每一个主机的通信，确保每个分组送往正确的地址。同时使用 NAT 的网络，与外部网络的连接只能由内部网络发起，极大地提高了内部网络的安全性。

NAT 的另一个显而易见的用途是解决 IP 地址匮乏问题。

(6) 网关技术。由于是直接串联在网络之中,新一代防火墙必须支持用户在互联网互联的所有服务,同时还要防止与互联网服务有关的安全漏洞。因此,它能够用多种安全的应用服务器(包括 FTP、Finger、Mail、Ident、News、WWW 等)来实现网关功能。为确保服务器的安全性,对所有的文件和命令均要利用改变根系统调用(chroot)作物理上的隔离。在域名服务方面,新一代防火墙采用两种独立的域名服务器,一种是内部 DNS 服务器,主要处理内部网络的 DNS 信息,另一种是外部 DNS 服务器,专门用于处理机构内部向互联网提供的部分 DNS 信息。

(7) 安全服务器。为适应越来越多的用户向互联网上提供服务时对服务器保护的需要,新一代防火墙采用分别保护的策略对用户上网的对外服务器实施保护,它利用一张网卡将对外服务器作为一个独立网络处理,对外服务器既是内部网的一部分,又与内部网关完全隔离。这就是安全服务器网络(SSN, Security Server Network)技术,对 SSN 上的主机既可单独管理,也可设置成通过 FTP、Telnet 等方式从内部网上管理。

(8) 鉴别与加密。为了降低防火墙产品在 Telnet、FTP 等服务和远程管理上的安全风险,鉴别功能必不可少,新一代防火墙采用一次性使用的口令字系统来作为用户的鉴别手段,并实现了对邮件的加密。

(9) 定制服务。为满足特定用户的特定需求,新一代防火墙在提供众多服务的同时,还为用户定制提供支持,这类选项有通用 TCP、出站 UDP、FTP、SMTP 等类,如果某一用户需要建立一个数据库的代理,便可利用这些支持,方便设置。

(10) 审计和告警。新一代防火墙产品的审计和告警功能十分健全,日志文件包括一般信息、内核信息、核心信息、接收邮件、邮件路径、发送邮件、已收消息、已发消息、连接需求、已鉴别的访问、告警条件、管理日志、进站代理、FTP 代理、出站代理、邮件服务器、域名服务器等。告警功能会守住每一个 TCP 或 UDP 探寻,并能以发出邮件、声响等多种方式报警。此外新一代防火墙还在网络诊断,数据备份与保全等方面具有特色。

(11) 十三元组。十三元组表示为:  $A=\{\text{网络环境, 防火墙, 访问数据信息, 数据特征识别策略, 访问者身份信息, 访问者权限信息, 网络数据情况, 控制规则, 访问数据流向信息, 访问控制技术, 网络监控技术, 网络防御者, 防护系统安全}\}$ 。

### 3. 拓扑方案的选择

防火墙的部署有很多常用的做法,就整个安全系统而言,它们或多或少都具有一定的可行性。按照安全性由低到高的顺序排列这些方案,分为基本过滤路由器、经典的双路由器隔离区(DMZ, Demilitarized Zone)方案、状态化防火墙 DMZ 方案、现代三接口防火墙方案、多防火墙方案。

#### 1) 基本过滤路由器

最不安全的做法是内部网络和外部网络之间只存在一个过滤点,比如图 7-7 中的基本过滤路由器。过滤路由器根据基本的访问控制列表(ACL, Access Control List)进行过滤。

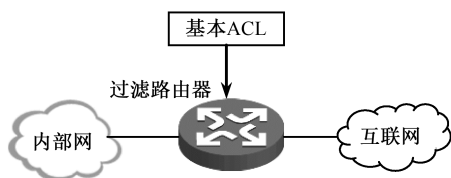


图 7-7 基本过滤路由器

这种设计有很多缺点。公共服务器位于路由器的内部，也就是说，如果公共服务器沦陷，那么攻击者就可以不经过路由器的过滤直接对内部系统发起攻击；仅部署一台过滤路由器执行访问控制存在单点故障的隐患；由于不能实现状态化过滤，因此必须在路由器上开放大量端口，才能让大部分应用正常工作。但这种过滤方案很容易实现。

## 2) 经典的双路由器 DMZ 方案

双路由器 DMZ 方案如图 7-8 所示。该方案的主要好处是，公共服务器与内部网的其余部分分开；一台服务器被攻陷并不会使得攻击者能够直接攻击内部服务器，它们必须经过第二台路由器才能进入内部。因此第二台过滤路由器可采用比第一台更严格的 ACL 策略进行设置，但是如果没有状态化过滤的功能，内部系统仍然面临攻击。

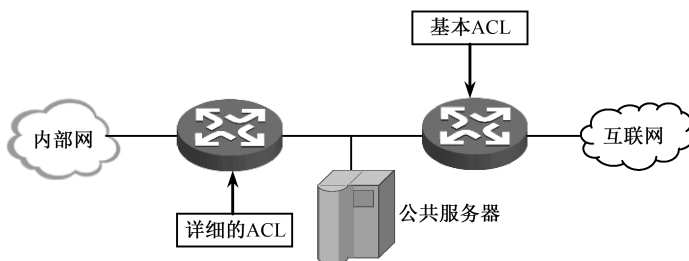


图 7-8 双路由器 DMZ 方案

## 3) 状态化防火墙 DMZ 方案

状态化防火墙 DMZ 方案如图 7-9 所示。该方案可以在内部网和公共服务器，以及内部网络和互联网之间执行更加强大的强过滤功能，因此是双路由器 DMZ 方案的改进做法。部署状态化防火墙时，网络的连通性可能会受到影响。有些防火墙不支持高级路由协议或多播功能，这在某些网络中可能是个问题；路由器仍然会执行某种过滤。

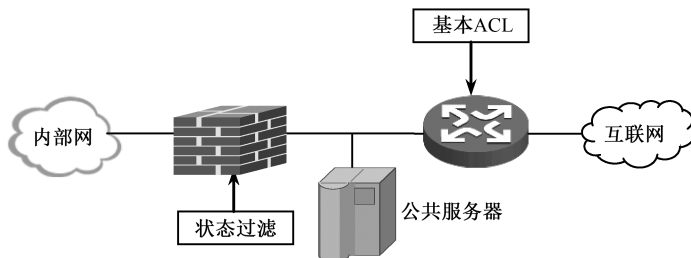


图 7-9 状态化防火墙 DMZ 方案

#### 4) 现代三接口防火墙方案

目前,大部分防火墙采用如图 7-10 所示的三接口防火墙方案。此方案成为当前防火墙边缘部署中的标准。还有更安全的选择(见下一种多防火墙方案),但此方案是安全性、经济性和易管理性的完美结合。这一方案所提供的最大优势是要求所有流量都经过防火墙,包括从互联网流向公共服务器的流量。另外还可以进行修改:可以在防火墙上添加更多的分段,将公共服务器相互隔离。

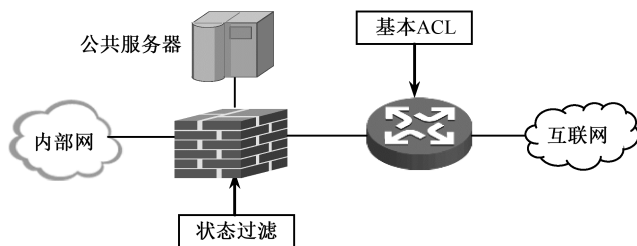


图 7-10 三接口防火墙方案

#### 5) 多防火墙方案

图 7-11 就是一个多防火墙方案的示例。在该方案中,信任服务器组通常会响应来自半信任服务器的业务请求。这些半信任服务器为来自非信任服务器的请求提供服务。非信任服务器则可以响应来自互联网的请求。而互联网用户只能直接访问非信任服务器。从非信任服务器上,可以攻击半信任服务器,但是只有极少数必要的端口支持这两台服务器之间的交互。如果半信任服务器被攻陷,那么信任服务器就可能从半信任服务器上被攻击,但是同样只有极少的端口可以发起攻击。有些专业人士提倡使用来自多家厂商的防火墙来提高网络的安全性。理由是即使一个防火墙存在某种漏洞,另一个则可能没有这个漏洞。

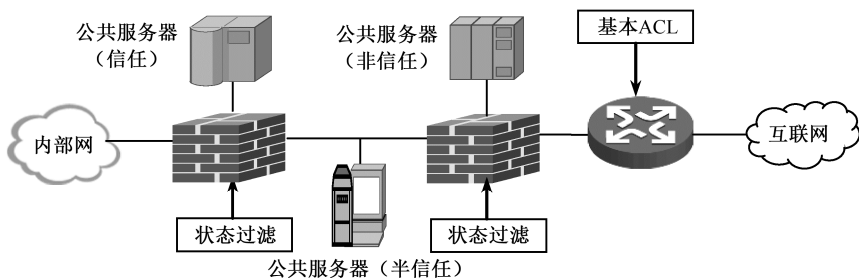


图 7-11 多防火墙方案

### 4. 防火墙选型要素

从产品角度来看,防火墙的选型主要考虑:①产品的综合性能,主要包括稳定性与可靠性、吞吐量、并发连接数、丢包率、延迟、缓存能力、有效通过率等性能参数指标;②产品的可管理性及功能方面,主要包括防火墙的可管理、状态检测、应用代理、支持

的服务类型、NAT、日志与报警、认证、带宽管理、联动等功能指标；③防火墙自身的安全性能方面，主要包括抗攻击能力、所采用的操作系统平台的安全性、抗毁能力、冗余能力等指标。

为较低的需求而采用高端的防火墙设备将造成投资的浪费，同样为较高的客户需求而采用低端设备将无法达到预期的性能指标。所以，从用户角度需要考虑：①厂家的研发力量、资金实力、企业的商业信誉和经营风险以及产品线的技术支持和售后服务体系等生产厂商的因素，要进行综合考虑；②要考虑用户实际网络安全性能的需求、业务系统、企业规模、发展空间、自身实力等，寻求投资和需求之间的平衡，选择合适的防火墙产品。

## 5. 防火墙技术的发展方向

从防火墙技术角度来看防火墙的发展，大致有以下几个发展方向：

- (1) 向具有安全操作系统的防火墙方向发展，以提高防火墙自身的安全性能；
- (2) 向高性能防火墙方向发展，以适应网络技术和带宽及基础设施的迅速发展；
- (3) 向防火墙功能的细化方向发展，即管理的通用化和产品的多样化。这是因为，各行各业的业务流是不同的，对防火墙的实际需求也会有差异，大而全的通用防火墙产品已不能很好地满足社会的实际需求，所以，防火墙将向功能细化方向发展；
- (4) 向防火墙与其他安全产品间的互操作方向发展，以实现网络安全产品之间的协同工作，充分发挥其安全保障性能；
- (5) 防火墙会向分布式防火墙方向发展，分布式配置、集中式配置管理和策略分发将满足网络技术的发展方向。

## 7.2.2 防病毒技术

CPU 内嵌的防病毒技术是一种硬件防病毒技术，与操作系统相配合，可以防范大部分针对缓冲区溢出漏洞的攻击（大部分是病毒）。Intel 的防病毒技术是删除禁用位（EDB, Excute Disable Bit），AMD 的防病毒技术是紧急病毒保护（EVP, Enhanced Virus Protection）。

### 1. 防病毒技术

从反病毒产品对计算机病毒的作用来讲，防毒技术可以直观地分为病毒预防技术、病毒检测技术及病毒清除技术。

#### (1) 病毒预防技术

计算机病毒预防技术就是通过一定的技术手段防止计算机病毒对系统的传染和破坏。实际上这是一种动态判定技术，即一种行为规则判定技术。计算机病毒预防是通过阻止计算机病毒进入系统内存或阻止计算机病毒对磁盘的操作，尤其是写操作。病毒预防技术包括磁盘引导区保护、加密可执行程序、读写控制技术、系统监控技术等。计算机病毒的预

防应用包括对已知病毒的预防和对未知病毒的预防两个部分。目前,对已知病毒的预防可以采用特征判定技术或静态判定技术,而对未知病毒的预防则是一种行为规则的判定技术,即动态判定技术。

### (2) 病毒检测技术

计算机病毒检测技术是指通过一定的技术手段判定出特定计算机病毒的一种技术。它有两种:一种是根据计算机病毒的关键字、特征程序段内容、病毒特征及传染方式、文件长度的变化,在特征分类的基础上建立的病毒检测技术。另一种是不针对具体病毒程序的自身校验技术,即对某个文件或数据段进行检验和计算并保存其结果,以后定期或不定期地以保存的结果对该文件或数据段进行检验,若出现差异,即表示该文件或数据段完整性已遭到破坏,感染上了病毒,从而检测到病毒的存在。

### (3) 病毒清除技术

目前,清除病毒大都是在某种病毒出现后,通过对其进行分析研究而研制出来的具有相应解毒功能的软件。这类软件技术发展往往是被动的,带有滞后性。而且由于计算机软件所要求的精确性,解毒软件有其局限性,对有些变种病毒的清除无能为力。

计算机病毒防范,是指通过建立合理的计算机病毒防范体系和制度,及时发现计算机病毒侵入,并采取有效的手段阻止计算机病毒的传播和破坏,恢复受影响的计算机系统和数据。它包括基于硬件的病毒防护和基于软件的病毒防护。我们日常生活中最常接触的杀毒软件就属于病毒防护设备,另外还包括病毒防火墙、硬件杀毒模块等设备。病毒的变异速度很快,种类繁多,这也决定了病毒防治是一项复杂的技术。

## 2. 计算机病毒检测方法

(1) 比较法,用原始备份与被检测引导扇区或文件做比较,看长度和内容变化。此种方法比较简便,不需专用软件,但无法确认病毒的种类名称。

(2) 加总比对法,将每个程序的文件名、大小、时间、日期及内容,加总为一个检查码,附于程序后;再利用此对比系统,追踪记录每个程序的检查码是否遭更改,判断是否感染病毒。

(3) 搜索法,用每一种病毒体含有的特定字符串对被检测的对象进行扫描。如果在对象内部发现了某一种特定字节串,就表明发现了该字节串所代表的病毒。缺点:①扫描费时;②特征串不易选;③特征库需要不断升级;④对变种病毒低效;⑤易产生误报;⑥难识别多维变形病毒。但它仍是今天用得最普遍的查毒方法。

(4) 人工智能陷阱法,这是监测计算机行为的常驻式扫描法。它将所有病毒产生的行为归纳起来,一旦发现内存中的程序有任何不当行为,系统就会有所警觉,并告知使用者。优点:速度快、操作简便,可侦测到各式病毒。缺点:程序设计难,且不易考虑周全。

(5) 宏病毒陷阱法,该技术结合了搜索法和人工智能陷阱法,依靠行为模式来侦测已知及未知的宏病毒。其中,配合 OLE2 [对象连接与嵌入 (OLE, Object Linking and Embedding)] 技术,可将宏与文件分开,使得扫描速度变得飞快,而且还可有效地将宏病毒彻底清除。

(6) 软件仿真扫描法，专门用来对付多态变形病毒。该病毒在每次传染时，都将自身以不同的随机数加密于每个感染的文件中，传统搜索法根本就无法找到它。软件仿真技术则是成功地仿真 CPU 执行，在 DOS 虚拟机下伪执行病毒程序，安全并确实地将其解密，使其显露本来的面目，再加以扫描。

(7) 先知扫描法，该技术将专业人员用来判断程序是否存在病毒代码的方法，分析归纳成专家系统和知识库，再利用软件模拟技术伪执行新的病毒，超前分析出新病毒代码，对付以后的病毒。

(8) 特征值扫描法，通过一一对比被检程序与病毒库中的特征值，来判断该目标是否被病毒感染。缺点：被动性、滞后性，免清除简单。黑客们只需经过修改病毒特征值，加壳等简单操作，就能够避免特征扫描的检测。

(9) 虚拟机检测法，在系统上虚拟一个操作环境，然后在这个虚拟环境下运行待检软件，在病毒现出原形后将其清除。

(10) 启发式检测法，采用智能启发式算法，分析文件代码逻辑结构所含有的病毒特征，或者通过在虚拟安全环境中执行代码，根据程序行为判断是否存在病毒。

(11) 沙盒检测法，使用病毒防御 API 相关的所有行为，使本机系统成为一个“沙盒”，让程序在“沙盒”中充分运行，当病毒真正出现后，对其进行清除，然后“沙盒”执行“回滚”机制，对病毒留下的痕迹进行彻底清除，让系统回复到原来的正常状态。

(12) 云安全检测法，通过网状的大量客户端对网络中软件异常行为进行监测，获取互联网中木马等病毒的最新信息，并传送到服务器端进行自动分析和处理，在每个客户端都设置病毒的解决方案，使整个互联网成为一个巨大的“杀毒软件”。

### 3. 病毒防范措施

“预防为主，治疗为辅”完全适合于对计算机病毒的处理。下面介绍一系列被实践证明行之有效的病毒预防措施。

(1) 新购置的计算机中可能携带病毒。建议对其用病毒检测软件检查是否有已知病毒，用人工检测的方法检查是否有未知病毒。在确保没有病毒之后，再使用新计算机。

(2) 新购置的硬盘或出厂时已格式化好的软盘可能有病毒。对硬盘可以进行检测或进行低级格式化，对硬盘只做 DOS 的 format 高级格式化不能消除主引导区（分区表扇区）病毒。对软盘做 DOS 的 format 格式化可以消除病毒。

(3) 新购置的计算机软件也要进行病毒检测。有些著名软件厂商在发售软件时，软件已被病毒感染或存储软件的软盘已受感染，这在国内外都是有先例的。

(4) 在保证硬盘无毒的情况下，尽量不要用软盘去启动。在不联网的情况下，软盘是传染病毒的最主要渠道。

(5) 提高使用计算机的安全意识。①避免链接形式进入密码网站。对于银行业务、网上交易、重要业务尽量不用链接的直接进入方式操作。要设置安全的密码，不要将设置的密码告诉其他人，并且经常更改密码以更好地保护计算机安全。②避免使用不确定的移动设备。③陌生网站或邮件尽量避免浏览，很多病毒或木马都是利用电子邮件进行传播的；



④抵制不良网站的诱惑，不落入病毒的陷阱。

(6) 安装正版杀毒软件和防火墙。安装有效的防毒软件是计算机防御系统的重要组成部分。在外网专设一台服务器，安装服务器版网络防杀病毒软件，对整个网络进行实时监控。它可以排除病毒对计算机的威胁，保护系统，保护自己的个人隐私。在因特网接入口处要安装防火墙式防杀病毒产品，在计算机上设置防火墙可以避免计算机受到恶意的攻击，它能够阻止内部网和外部网之间的任何活动，从而保证内部网络的安全。

(7) 及时更新系统并合理安装软件程序。①及时更新查杀计算机病毒引擎，一般至少一个月更新一次，最好每周更新一次，如果遇到突发病毒应及时更新；②经常用杀毒软件对系统进行病毒检查和清除（常见病毒防御软件有比特梵德、瑞星、诺顿、360、江民、金山、卡巴斯基、腾讯电脑管家等）；③不要在安全性得不到保障的网站下载软件；④不随意下载安全不知晓的软件；⑤对外来软盘、光盘和网上下载的软件等都应先查杀病毒，然后使用；⑥安装正版防病毒软件，并经常升级；⑦病毒特征代码库要经常更新；⑧安装病毒实时监控程序；⑨安装软件程序时，要合理、谨慎地选择某些功能模块；⑩随时对电脑所不需要的东西进行清理，适时地进行检查、杀毒等一些措施，以防止病毒残留；⑪及时修补软件漏洞；⑫利用病毒防御软件清除病毒。

(8) 正确使用移动设备。使用 U 盘时，最好先进行病毒查杀；禁止用 U 盘自动播放。

(9) 设置安全密码，并对数据加密。建议设置长度在 8 位以上的密码，最好采用英文、数字、特殊符号等组合方式。数据加密一般利用某种算法，对原有数据加密并转换，把正在进行的存储及传输工作加密，在相关使用者解密以后方可使用数据。

(10) 数据备份与权限设置。操作系统和数据文件放置在不同的分区，对存储的文件数据定期备份，以便被病毒攻击后能够及时恢复数据，将损失降到最小。除此之外，可以将操作系统做成镜像文件，在感染病毒使得系统崩溃时可以及时将系统恢复正常。为了防止文件型病毒对用户造成威胁，在不影响正常工作的前提下对系统文件设置访问权限，如修改、改名、删除、创建、只读和写文件等操作权限。

(11) 在 Word 中将“宏病毒防护”选项打开，并打开“提示保存 Normal 模板”，退出 Word，将 Normal.dot 文件的属性改成只读。

(12) 在 Excel 和 PowerPoint 中将“宏病毒防护”选项打开。

(13) 若用 Outlook Express 收发电子邮件，应关闭信件预览功能。

(14) 在 IE 或 Netscape 等浏览器中设置合适的因特网安全级别，防范来自 ActiveX 和 Java Applet 的恶意代码。

(15) 采用工作站防毒芯片。将防毒功能集成到一个芯片上，在网络工作stations上安装该芯片，从而达到对工作站的保护。

(16) 一定要用硬盘启动网络服务器，否则在受到引导型计算机病毒感染和破坏后，遭受损失的将不是一个人的机器，而会影响整个网络的中枢。

(17) 实时在线扫描服务器中所有文件。24 小时监控服务器中的文件是否带有病毒并给予对应的处理方法。

(18) 开放用户特征接口。对用户在工作过程中遇到的带毒文件，可对病毒进行特征分析并自动将该特征加入特征库中，增强服务器的抗毒能力。

### 7.2.3 数据加密技术

#### 1. 概念

所谓数据加密（Data Encryption）技术是指将一个信息（或称明文）经过加密钥匙及加密函数转换，变成无意义的密文，而接收方则将此密文经过解密函数、解密钥匙还原成明文。它是一门通过数学或物理方法来改变数据信息表现形式，隐藏信息真实含义的技术。加密技术是网络安全技术的基石。

数据加密技术要求只有在指定的用户或网络下，才能解除密码而获得原来的数据，这就需要给数据发送方和接受方以一些特殊的信息用于加解密，这就是所谓的密钥。其密钥的值是从大量的随机数中选取的。

数据加密技术保障信息安全性的前提是计算机系统是安全的，加密技术关注数据传输过程的安全性。其十元组  $A$  表示如下：

$A = \{\text{网络环境, 数据加密系统, 密钥信息, 密钥信息, 保密能力信息, 数据传输路径, 终端系统安全性信息, 数据加密技术, 网络防御者, 防护数据安全}\}$ 。

数据加密技术在网络作战环境中应用十分广泛，如文件加密、数字证书、数字签名、信息隐藏与数字水印、信息的防泄露、信息源认证、信息防篡改、信息防否认、消息鉴别等，可以有效地保障数据的安全性和完整性。

#### 2. 分类

从不同的角度，根据不同的标准，可以把密码分成若干类。

(1) 按应用或发展阶段划分为手工密码、机械密码、电子机内乱密码和计算机密码。

① 手工密码。以手工完成加密作业，或者以简单器具辅助操作的密码，叫作手工密码。第一次世界大战前主要是这种作业形式。

② 机械密码。以机械密码机或电动密码机来完成加解密作业的密码，叫作机械密码。这种密码从第一次世界大战出现到第二次世界大战中得到普遍应用。

③ 电子机内乱密码。通过电子电路，以严格的程序进行逻辑运算，以少量制造混乱的元素生产大量的加密乱数，因为其制造混乱是在加解密过程中完成的而不需预先制作，所以称为电子机内乱密码。这种密码从 20 世纪 50 年代末期出现，到 20 世纪 70 年代得到广泛应用。

④ 计算机密码。它是以计算机软件编程进行算法加密为特点，适用于计算机数据保护和网络通信等广泛用途的密码。

(2) 按加密算法分为专用密钥和公开密钥两种。

① 专用密钥，又称为对称密钥或单密钥，加密和解密时使用同一个密钥，即同一个算法。如数据加密标准（DES, Data Encryption Standard）和 MIT（麻省理工学院）的 Kerberos 算法。单密钥是最简单的方式，通信双方必须交换彼此密钥，当需给对方发信息时，用自己的加密密钥进行加密，而在接收方收到数据后，用对方所给的密钥进行解密。当一个文

本要加密传送时,该文本用密钥加密构成密文,密文在信道上传送,收到密文后用同一个密钥将密文解出来,形成普通文本供阅读。在对称密钥中,密钥的管理极为重要,一旦密钥丢失,密文将无密可保。这种方式在与多方通信时因为需要保存很多密钥而变得很复杂,而且密钥本身的安全就是一个问题。

② 公开密钥,又称非对称密钥,加密和解密时使用不同的密钥,即不同的算法,虽然两者之间存在一定的关系,但不可能轻易地从一个推导出另一个。有一把公用的加密密钥,有多把解密密钥,如非对称加密算法(RSA, Rivest-Shamir-Adelman)。

非对称密钥由于两个密钥(加密密钥和解密密钥)各不相同,因而可以将一个密钥公开,而将另一个密钥保密,同样可以起到加密的作用。

在这种编码过程中,一个密码用来加密消息,而另一个密码用来解密消息。在两个密钥中有一种关系,通常是数学关系。公钥和私钥都是一组十分长的、数字上相关的素数(是另一个大数字的因数)。有一个密钥不足以翻译出消息,因为用一个密钥加密的消息只能用另一个密钥才能解密。每个用户可以得到唯一的一对密钥,一个是公开的,另一个是保密的。公共密钥保存在公共区域,可在用户中传递,甚至可印在报纸上面。而私钥必须存放在安全保密的地方。任何人都可以有你的公钥,但是只有你一个人能有你的私钥。它的工作过程是:你要我听你的吗?除非你用我的公钥加密该消息,我就可以听你的,因为我知道没有别人在偷听。只有我的私钥(其他人没有)才能解密该消息,所以我知道没有人能读到这个消息。我不必担心大家都有我的公钥,因为它不能用来解密该消息。

公开密钥的加密机制虽提供了良好的保密性,但难以鉴别发送者,即任何得到公开密钥的人都可以生成和发送报文。数字签名机制提供了一种鉴别方法,以解决伪造、抵赖、冒充和篡改等问题。

(3) 根据密码算法所使用的加密密钥和解密密钥是否相同或能否由一个密钥简单地推导出另一个,可将密码体制分为对称密钥密码体制和非对称密钥密码体制。

① 对称密钥是最古老的,一般说“密电码”采用的就是对称密钥。由于对称密钥运算量小、速度快、安全强度高,因而现在仍广泛采用。其常用的算法主要有 DES 系列算法、高级加密标准(AES, Advanced Encryption Standard)、RC 系列算法和国际数据加密算法(IDEA, International Data Encryption Algorithm)等。

DES 是一种数据分组的加密算法,它将数据分成长度为 64 位的数据块,其中 8 位用作奇偶校验,剩余的 56 位作为密码的长度。第一步将原文进行置换,得到 64 位的杂乱无章的数据组;第二步将其分成均等两段;第三步用加密函数进行变换,并在给定的密钥参数条件下,进行多次迭代而得到加密密文。

② 非对称加密技术。数字签名一般采用非对称加密技术(如 RSA),通过对整个明文进行某种变换,得到一个值,作为核实签名。接收者使用发送者的公开密钥对签名进行解密运算,如其结果为明文,则签名有效,证明对方的身份是真实的。当然,签名也可以采用多种方式,如将签名附在明文之后。数字签名普遍用于银行、电子贸易等。

数字签名不同于手写签字:数字签名随文本的变化而变化,手写签字反映某个人个性特征,是不变的;数字签名与文本信息是不可分割的,而手写签字是附加在文本之后的,

与文本信息是分离的。

值得注意的是，能否切实有效地发挥加密机制的作用，关键的问题在于密钥的管理，包括密钥的生存、分发、安装、保管、使用和作废全过程。

非对称密码体制主要基于数学难题而产生，其常用的算法主要有 RSA 算法、椭圆曲线加密（ECC，Elliptic Curves Cryptography）算法和 ElGama 算法等。

（4）按明文形态划分模拟型密码和数字型密码。

① 模拟型密码，用以加密模拟信息。如对动态范围之内，连续变化的语音信号加密的密码，叫作模拟式密码。

② 数字型密码，用于加密数字信息。对两个离散电平构成 0、1 二进制关系的电报信息加密的密码，叫作数字型密码。

### 3. 加密技术

密码技术是网络安全最有效的技术之一。一个加密网络，不但可以防止非授权用户的搭线窃听和入网，而且也是对付恶意软件的有效方法之一。一般的数据加密可以在通信的三个层次来实现：链路加密、节点加密和端到端加密。

#### 1) 链路加密

对于在两个网络节点间的某一次通信链路，链路加密能为网上传输的数据提供安全保证。对于链路加密（又称在线加密），所有消息在被传输之前就进行加密，在每一个节点对接收到消息进行解密，然后先使用下一个链路的密钥对消息进行加密，再进行传输。在到达目的地之前，一条消息可能要经过许多通信链路的传输。

由于在每一个中间传输节点消息均被解密后重新进行加密，因此，包括路由信息在内的链路上的所有数据均以密文形式出现。这样，链路加密就掩盖了被传输消息的源点与终点。由于填充技术的使用以及填充字符在不需要传输数据的情况下就可以进行加密，这使得消息的频率和长度特性得以掩盖，从而可以防止对通信业务进行分析。

尽管链路加密在网络环境中使用得相当普遍，但它并非没有问题。链路加密通常用在点对点的同步或异步线路上，它要求先对在链路两端的加密设备进行同步，然后使用一种模式对链路上传输的数据进行加密。这就给网络的性能和可管理性带来了副作用。

在线路/信号经常不通的海外或卫星网络中，链路上的加密设备需要频繁地进行同步，带来的后果是数据丢失或重传。另一方面，即使仅一小部分数据需要进行加密，也会使得所有传输数据被加密。

在一个网络节点，链路加密仅在通信链路上提供安全性，消息以明文形式存在，因此所有节点在物理上必须是安全的，否则就会泄露明文内容。然而保证每一个节点的安全性需要较高的费用，为每一个节点提供加密硬件设备和一个安全的物理环境所需要的费用由以下几部分组成：保护节点物理安全的雇员开销，为确保安全策略和程序的正确执行而进行审计时的费用，以及为防止安全性被破坏时带来损失而参加保险的费用。

在传统的加密算法中，用于解密消息的密钥与用于加密的密钥是相同的，该密钥必须

被秘密保存,并按一定规则进行变化。这样,密钥分配在链路加密系统中就成了一个问题,因为每一个节点必须存储与其相连接的所有链路的加密密钥,这就需要对密钥进行物理传送或建立专用网络设施。而网络节点地理分布的广阔性使得这一过程变得复杂,同时增加了密钥连续分配时的费用。

### 2) 节点加密

不仅节点加密能给网络数据提供较高的安全性,而且它在操作方式上与链路加密是类似的:两者均在通信链路上为传输的消息提供安全性;都在中间节点先对消息进行解密,然后进行加密。因为要对所有传输的数据进行加密,所以加密过程对用户是透明的。然而,与链路加密不同,节点加密不允许消息在网络节点以明文形式存在,它先把收到的消息进行解密,然后采用另一个不同的密钥进行加密,这一过程是在节点上的一个安全模块中进行。

节点加密要求报头和路由信息以明文形式传输,以便中间节点能得到如何处理消息的信息。因此,这种方法对于防止攻击者分析通信业务是脆弱的。

### 3) 端到端加密

端到端加密允许数据在从源点到终点的传输过程中始终以密文形式存在。采用端到端加密,消息在被传输时到达终点之前不进行解密,因为消息在整个传输过程中均受到保护,所以即使有节点被损坏也不会使消息泄露。

端到端加密系统的价格便宜,并且与链路加密和节点加密相比更可靠,更容易设计、实现和维护。端到端加密还避免了其他加密系统所固有的同步问题,因为每个报文包均是独立被加密的,所以一个报文包所发生的传输错误不会影响后续的报文包。此外,从用户对安全需求的直觉上讲,端到端加密更自然。单个用户可能会选用这种加密方法,以便不影响网络上的其他用户,此方法只需要源和目的节点是保密的即可。

端到端加密系统通常不允许对消息的目的地址进行加密,这是因为每一个消息所经过的节点都要用此地址来确定如何传输消息。由于这种加密方法不能掩盖被传输消息的源点与终点,因此它对于防止攻击者分析通信业务是脆弱的。

## 4. 数据加密的一般模型

数据加密的一般模型如图 7-12 所示,明文  $P$  用加密算法  $E$  和加密密钥  $K$  得到密文  $C=E_K(P)$ 。在传送过程中可能出现密文截取者。到了收端,利用解密算法  $D$  和解密密钥  $K$ ,解出明文为  $D_K(C)=D_K[E_K(P)]=P$ 。截取者又称为攻击者,或入侵者。在这里假定加密密钥和解密密钥都是一样的。但实际上它们可以是不一样的(即使不一样,这两个密钥也必然有某种相关性)。密钥通常是由一个密钥源提供。当密钥需要向远的地方传送时,一定要通过另一个安全通道。

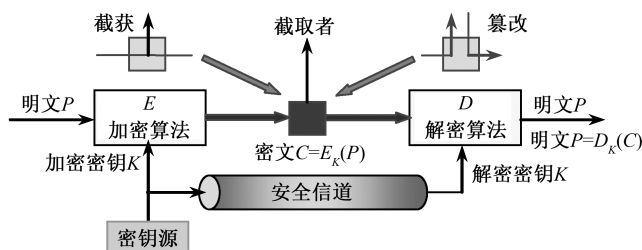


图 7-12 数据加密的一般模型

## 7.2.4 信息隐藏技术

### 1. 含义

信息隐藏，或称信息伪装技术，是将秘密信息伪装隐藏于普通的文件中，然后再通过网络传递散发出去，使其不被他人发现，从而实现隐蔽通信或隐蔽标志。信息隐藏技术，简单地说，主要是指将特定的信息（指示、命令、决心、态势图等）隐藏在数字化宿主信息中的方法。被隐藏的秘密信息可以是文字、密码、图像、图形或声音。隐藏方法主要有图像中的信息隐藏、音频中的信息隐藏和文本中的信息隐藏等几种。它与密码技术有密切联系，但两者的作用完全不同。信息隐藏技术要求具有鲁棒性、不可检测性、透明性、安全性和自恢复性等。其研究范围则涉及密码学、图像处理、模式识别、数学和计算机科学等领域。信息隐藏技术在保护信息的完整性、机密性和可用性等方面发挥了重要作用，较之单纯的密码加密更多了一层保护，使得网络加密机制从“看不懂”变为“看不见”，从而不成为好事者攻击的目标。目前的信息隐藏技术主要有数字水印技术、隐写术、隐匿协议等。

### 2. 基本原理

信息隐藏是集多种理论与技术于一身的新兴技术领域，是利用人类感觉器官对数字信号的感觉冗余，将一个有意义的信息（称为待隐消息或秘密消息）如软件序列号、秘文或版权信息等内容通过某种嵌入算法隐藏到另一个信息（称为遮掩消息或载体）中，从而得到隐秘载体的过程。

信息隐藏的目的不是限制资料信息的交流存取，而在于保证隐藏的信息不引起攻击者的注意、重视和破坏。信息隐藏不但隐藏了信息的内容而且隐藏了信息的存在，从而减少被侵犯的可能性，在此基础上再使用密码学中的经典方法来加强隐藏信息的安全性，可以起到保护信息安全的作用。

### 3. 在部队作战中的应用

信息隐藏技术在网络空间作战中的应用,可以通过 C<sup>4</sup>ISR 系统利用文本、数字化的声音、图像等信息作为媒体,对作战指挥的机密信息进行隐藏传输,以防信息失密而贻误战机。

信息隐藏技术在军事上的应用,可以将一些不愿为人所知的重要标志信息用信息隐藏的方式进行隐蔽存储,像军事地图中标明的军备部署、打击目标,卫星遥感图像的拍摄日期、经纬度等,都可用隐藏标记的方法使其以不可见的形式隐藏起来,只有掌握识别软件的人才能读出标记所在。

### 4. 模型

信息隐藏系统的一般模型如图 7-13 所示,主要包括信息嵌入算法和隐蔽信息检测/提取算法两个模块。信息嵌入算法利用对称密钥或公开密钥来实现秘密信息的隐藏,得到隐秘载体。隐蔽信息检测/提取算法利用相应的密钥从隐蔽载体中检测或恢复出秘密信息。没有解密密钥,攻击者很难从隐秘载体中发现和编辑秘密信息。

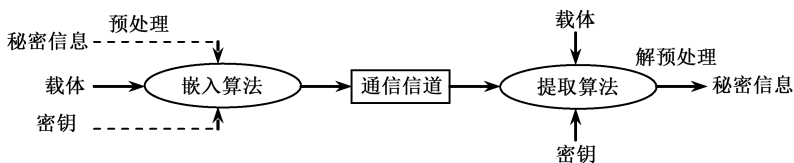


图 7-13 信息隐藏系统的一般模型

### 5. 信息隐藏关键技术

近年来,已经提出了各种各样的隐藏算法。关键的信息隐藏技术有以下 3 种。

#### 1) 替换技术

所谓替换技术,就是试图用秘密信息比特替换掉伪装载体中不重要的部分,以达到对秘密信息进行编码的目的。替换技术包括最不重要比特位 (LSB, The Least Significant Bits) 替换、最低比特位替换、伪随机替换、载体区域的奇偶校验位替换和基于调色板的图像替换等。替换技术是在空间域进行的一种操作,通过选择合适的伪装载体和适当的嵌入区域,能够有效地嵌入秘密信息比特,同时又可保证数据的失真度在人的视觉允许范围内。比如利用 LSB 算法可以在 8 色、16 色、256 色以及 24 位真彩色图像中隐藏信息。对于 256 色图像,在不考虑压缩的情况下,每个字节存放 1 个像素点,那么 1 个像素点至少可隐藏 1 位信息,1 幅  $640 \times 480$  的 256 色图像至少可隐藏  $640 \times 480 = 307\,200$  位的信息。对于 24 位真彩色图像,在不考虑压缩的情况下,3 个字节存放 1 个像素点,那么 1 个像素点至少可隐藏 3 位信息,1 幅  $1024 \times 768$  的 24 位真彩色图像至少可隐藏  $1024 \times 768 \times 3 = 2\,359\,296$  位的信息。

## 2) 变换技术

大部分信息隐藏算法都是在变换域进行的，其变换技术包括离散傅里叶变换（DFT，Discrete Fourier Transform）、离散余弦变换（DCT，Discrete Cosine Transform）、离散小波变换（DWT，Discrete Wavelet Transform）和离散哈达玛特变换（DHT，Discrete Hadamard Transform）等。这些变换技术都有各自的特点。DFT 将图像分割成多个感觉频段，然后选择合适部分来嵌入秘密信息。DCT 使空间域的能量重新分布，通常在一个图像块中调整两个（或多个）DCT 系数的相对大小。DWT 是对图像的一种多尺度、空间-频率分解，即将输入信号分解为低分辨率参考信号和一系列细节信号。DHT 是对信号的一种正交变换，将图像由常规空域转换到相应的变换域，用于对图像本质特征的分析，在图像增强、恢复、编码、描述和特征提取等方面有广泛的应用。

现以 DCT 变换域数字水印算法为例进行说明，其嵌入过程如图 7-14 所示。原图像在经过 DCT 变换以后，插入水印。一方面得到水印信息，另一方面经过逆离散余弦变换（IDCT，Inverse DCT），变换以后得到嵌入水印的图像。



图 7-14 基于 DCT 变换的数字水印嵌入过程

## 3) 扩频技术

当对伪装对象进行过滤操作时可能会消除秘密信息，解决的方法就是重复编码，即扩展隐藏信息。在整个伪装载体中多次嵌入一个比特，使得隐藏信息在过滤后仍能保留下来，这种方法虽然传输效率不高，但却具有较好的健壮性。扩频技术一般使用比发送的信息数据速率高许多倍的伪随机码，将载有信息数据的基带信号频谱进行扩展，形成宽带低功率谱密度信号。最典型的扩频技术为直序扩频和跳频扩频。直序扩频是在发送端直接用具有高码率的扩频编码去扩展信号的频谱，而在接收端用相同的扩频编码解扩，将扩频信号还原为原始信号。跳频扩频是在发端将信息码序列与扩频码序列组合，然后按照不同的码字去控制频率合成器，使输出频率根据码字的改变而改变，形成频率的跳变；在接收端为了解跳频信号，要用与发送端完全相同的本地扩频码发生器去控制本地频率合成器，从中恢复出原始信息。

## 6. 信息隐藏的方法

信息隐藏的方法主要有：

（1）利用扩展频谱通信传递信息。扩展频谱通信就是将待传送的信息数据用伪随机编码调制，实现频谱扩展后再传输，接收端采用同样的编码进行解调和相关处理，恢复原始信息数据。在作战指挥过程中利用这种信息隐藏技术，将消息拆分成简短的连续部分，把集中于较窄频段的待传送信息扩展到较宽频带，通过一个预先安排好的频率序列发送出



去,实现信息在更广泛的频率带宽上进行传输,达到隐蔽通信的目的。

(2) 利用流星猝发通信传递信息。利用微流星体电离轨迹进入地球大气层时反射无线电波的特性建立的通信称为流星猝发通信,具有轨迹迅速散射、信号强度快速衰减等特征,在作战信息传达过程中,利用流星猝发通信传递信息,可达到信息隐藏的目的。

(3) 利用文本文件传递信息。信息传输过程中,将秘密信息经加密后嵌入到所选定的文本(该文本本身不包含秘密信息,不应引起敌方的注意)中,通过选定的传输线路将伪装对象传递给接收方。接收方利用相应的密钥把秘密信息提取出来,从而实现隐蔽通信。

(4) 利用视频通信传递信息。在利用视频通信系统进行秘密通信时,发送方将秘密信息经过加密嵌入到所选定的视频流中,通过选定的传输线路将伪装对象传递给接收方。接收方利用相应的密钥把秘密信息提取出来,从而实现隐蔽通信。

(5) 利用图像、数字声音传递信息。在用图像、数字声音传递秘密信息时,发送方将秘密信息经过加密嵌入到所选定的图像、数字声音文件的噪声成分中,通过传输路线将伪装对象传递给接收方。接收方利用相应的密钥把秘密信息提取出来,从而实现隐蔽通信。

此外,为了控制秘密信息在系统中的访问权限和防止秘密信息意外丢失、泄密,必须对密钥的使用进行严格的控制。对于不同密级的信息在嵌入伪装载体时采用不同的密钥,同时对于不同的用户根据其访问权限赋予不同的密钥。

## 7.2.5 访问控制技术

### 1. 基本概念

访问是使信息在主体和对象间流动的一种交互方式。主体是指主动的实体,该实体造成了信息的流动和系统状态的改变,主体通常包括人、进程和设备。对象是指包含或接受信息的被动实体,通常包括记录、块、页、段、文件、目录、目录树和程序,以及位、字节、字、字段、处理器、显示器、键盘、时钟、打印机和网络节点。控制是为了达成既定的目的和目标而采取的行动。

访问控制是指确定用户权限以及实施访问权限的过程,主要为了防止越权使用资源或非法用户的访问。通过限制对关键资源的访问,防止非法的主体进入受保护的网路资源;允许合法用户访问受保护的网路资源;防止合法的用户对受保护的网路资源进行非授权的访问;保证网路资源受控、合法地使用。

访问控制的手段包括用户识别代码、口令、登录控制、资源授权(如用户配置文件、资源配置文件和控制列表)、授权核查、日志和审计。

### 2. 访问控制的类型

主要的访问控制类型有:自主访问控制、强制访问控制、基于角色的访问控制、基于

对象的访问控制和基于任务的访问控制。

### 1) 自主访问控制 (DAC, Discretionary Access Control)

DAC 是一种接入控制服务, 通过执行基于系统实体身份及其系统资源的接入授权。包括在文件、文件夹和共享资源中设置许可。用户有权对自身所创建的文件、数据表等访问对象进行访问, 并可将其访问权授予其他用户或收回其访问权限。允许访问对象的属主制定针对该对象访问的控制策略, 可通过访问控制列表来限定针对客体可执行的操作。

DAC 提供了适合多种系统环境的灵活方便的数据访问方式, 是应用最广泛的访问控制策略。然而, 它所提供的安全性可被非法用户绕过, 授权用户在获得访问某资源的权限后, 可能传送给其他用户。主要是在自主访问策略中, 用户获得文件访问后, 不限制对该文件信息的操作, 即没有限制数据信息的分发。所以 DAC 提供的安全性相对较低, 无法对系统资源提供严格保护。

### 2) 强制访问控制 (MAC, Mandatory Access Control)

MAC 是系统强制主体服从访问控制策略, 由系统对用户所创建的对象, 按照规定的规则控制用户权限及操作对象的访问。主要特征是对所有主体及其所控制的进程、文件、段、设备等客体实施强制访问控制。

在 MAC 中, 每个用户及文件都被赋予一定的安全级别, 只有系统管理员才可确定用户和组的访问权限, 用户不能改变自身或任何客体的安全级别。MAC 的安全级别有多种定义方式, 常用的分为 5 级: 绝密级、秘密级、机密级、限制级和无级别级。越是靠前的密级越高, 越是靠后的密级越低。所有系统中的主体 (用户, 进程) 和客体 (文件, 数据) 都分配安全标签, 以标志安全等级。系统通过比较用户和访问文件的安全级别, 决定用户是否可以访问该文件。

MAC 可通过使用敏感标签对所有用户和资源强制执行安全策略, 一般采用 3 种方法: 限制访问控制、过程控制和系统限制。MAC 常用于多级安全军事系统, 对专用或简单系统较有效, 但对通用或大型系统并不太有效。

### 3) 基于角色的访问控制 (RBAC, Role-Based Access Control)

角色是一定数量的权限的集合, 指完成一项任务必须访问的资源及相应操作权限的集合。RBAC 是将访问许可权分配给一定的角色, 用户通过饰演不同的角色获得角色所拥有的访问许可权。角色由系统管理员定义, 角色成员的增减也只能由系统管理员来执行, 即只有系统管理员有权定义和分配角色。用户与客体无直接联系, 他只有通过角色才享有该角色所对应的权限, 从而访问相应的客体。因此用户不能自主地将访问权限授给别的用户。RBAC 减小了授权管理的复杂性, 降低管理开销, 提高了网络安全策略的灵活性。

RBAC 模型的授权管理方法主要有 3 种: ①根据任务需要定义具体不同的角色; ②为不同角色分配资源和操作权限; ③给一个用户组 (权限分配的单位与载体) 指定一个角色。RBAC 支持三个著名的安全原则: 最小权限原则、责任分离原则和数据抽象原则。

#### 4) 基于对象的访问控制 (OBAC, Object-Based Access Control)

控制策略和控制规则是 OBAC 访问控制系统的核心所在, OBAC 将访问控制列表与受控对象或受控对象的属性相关联, 并将访问控制选项设计成为用户、组或角色及其对应权限的集合; 允许对策略和规则进行重用、继承和派生操作。

这样, 不仅可以对受控对象本身进行访问控制, 受控对象的属性也可以进行访问控制, 而且派生对象可以继承父对象的访问控制设置, 这对于信息量巨大、信息内容更新变化频繁的管理信息系统非常有益, 可以减轻由于信息资源的派生、演化和重组等带来的分配、设定角色权限等的工作量。

OBAC 访问控制系统是从信息系统的差异变化和用户需求出发, 有效地解决了信息数据量大、数据种类繁多、数据更新变化频繁的大型管理信息系统的安全管理; 并从受控对象的角度出发, 将访问主体的访问权限直接与受控对象相关联。一方面, 定义对象的访问控制列表, 增、删、修改访问控制项易于操作; 另一方面, 当受控对象的属性发生改变, 或者受控对象发生继承和派生行为时, 无须更新访问主体的权限, 只需要修改受控对象的相应访问控制项即可, 从而减少了访问主体的权限管理, 降低了授权数据管理的复杂性。

#### 5) 基于任务的访问控制 (TBAC, Task-Based Access Control)

基于任务的访问控制是从应用和工作流角度来解决安全问题, 以面向任务的观点, 从任务 (活动) 的角度来建立安全模型和实现安全机制, 在任务处理的过程中提供动态实时的安全管理和权限管理。

在 TBAC 中, 对象的访问权限控制并不是静止不变的, 而是随着执行任务的上下文环境发生变化。首先, TBAC 考虑的是在工作流的环境中对信息的保护问题。在工作流环境中, 数据的处理与上一次的处理相关联, 相应的访问控制也如此, 因而 TBAC 是一种上下文相关的访问控制模型。其次, TBAC 不仅能对不同工作流实行不同的访问控制策略, 而且还能对同一工作流的不同任务实例实行不同的访问控制策略。从这个意义上说, TBAC 是基于任务的, 这也表明, TBAC 是一种基于实例的访问控制模型。

TBAC 模型由工作流、授权结构体、受托人集、许可集四部分组成。它一般用五元组 (S, O, P, L, AS) 来表示, 其中 S 表示主体, O 表示客体, P 表示许可, L 表示生命周期, AS 表示授权步。授权步 (Authorization Step) 表示一个原始授权处理步, 是指在一个工作流程中对处理对象的一次处理过程。授权步是访问控制所能控制的最小单元, 由受托人集合多个许可集组成。由于任务都是有时效性的, 所以在基于任务的访问控制中, 用户对于授予他的权限的使用也是有时效性的。TBAC 非常适合分布式计算和多点访问控制的信息处理控制, 以及在工作流、分布式处理和事务管理系统中的决策制定。

### 3. 安全策略的实施原则

安全策略的制定实施是围绕主体、客体和访问控制规则三者之间的关系展开的。

(1) 最小特权原则。最小特权原则是指主体执行操作时，按照主体所需权力的最小化原则分配给主体权力。也就是说，为了达到一定目的，主体必须执行一定操作，但他只能做他所被允许做的，其他除外。

(2) 最小泄露原则。最小泄露原则是指主体执行任务时，按照主体所需要知道的信息最小化的原则分配给主体权力。

(3) 多级安全策略。多级安全策略是指主体和客体间的数据流向和权限控制，按照安全级别的绝密、秘密、机密、限制和无级别五级来划分。

#### 4. 访问控制技术

访问控制技术所涉及内容较为广泛，包括网络登录控制、网络使用权限控制、目录级安全控制，以及属性安全控制等多种手段。

##### 1) 网络登录控制

网络登录控制是网络访问控制的第一道防线。通过网络登录控制可以限制用户对网络服务器的访问，或禁止用户登录；限制用户只能在指定的工作站和指定的时间进行登录，或登录到指定的服务器上。

网络登录控制一般需要经过三个环节，一是验证用户身份，识别用户名；二是验证用户口令，确认用户身份；三是核查该用户账号的默认权限。在这三个环节中，只要其中一个环节出现异常，该用户就不能登录网络。

网络登录控制是由网络管理员依据网络安全策略实施的。网络管理员可以随时建立或删除普通用户账号，可以控制和限制普通用户账号的活动范围、访问网络的时间和访问方式，并对登录过程进行必要的审计。对于试图非法登录网络的用户，一经发现立即报警。

##### 2) 网络使用权限控制

当用户成功登录网络后，就可以使用其所拥有的权限对网络资源（如目录、文件和相应设备等）进行访问。通过网络使用权限控制可以规范和限制用户对网络资源的访问，允许用户访问的资源就开放给用户，不允许用户访问的资源一律加以控制和保护。

网络使用权限控制是通过访问控制表来实现的。在这个访问控制表中，规定了用户可以访问的网络资源，以及能够对这些资源进行的操作。根据网络使用权限，可以将网络用户分为三大类：一是系统管理员用户，负责网络系统的配置和管理；二是审计用户，负责网络系统的安全控制和资源使用情况的审计；三是普通用户，这是由系统管理员创建的用户，其网络使用权限是由系统管理员根据他们的实际需要授予的。系统管理员可随时更改普通用户的权限，或将其删除。

### 3) 目录级安全控制

目录级安全控制主要是为了控制用户对目录、文件和设备的访问,或指定对目录下的子目录和文件的使用权限。用户在目录一级制定的权限对所有目录下的文件仍然有效,还可进一步指定子目录的权限。在网络和操作系统中,有系统管理员权限、读权限、写权限、创建权限、删除权限、修改权限、文件查找权限、控制权限等。一个网络管理员应为用户分配适当的访问权限,以控制用户对服务器资源的访问,进一步强化网络和服务器的安全。

### 4) 属性安全控制

属性安全控制可将特定的属性与网络服务器的文件及目录网络设备相关联。在权限安全的基础上,对属性安全提供更进一步的安全控制。网络上的资源都应先标示其安全属性,将用户对应网络资源的访问权限存入访问控制列表中,记录用户对网络资源的访问能力,以便进行访问控制。

属性安全控制包括向某个文件写数据、复制一个文件、删除目录或文件、查看目录和文件、执行文件、隐含文件、共享、系统属性等。安全属性可以保护重要的目录和文件,防止用户越权对目录和文件的查看、删除和修改等。

### 5) 网络服务器安全控制

网络服务器安全控制允许通过服务器控制台执行的安全控制操作,包括用户利用控制台装载和卸载操作模块、安装和删除软件等。操作网络服务器的安全控制还包括设置口令锁定服务器控制台,主要防止非法用户修改、删除重要信息或破坏数据。另外,系统管理员还可通过设定服务器的登入时间限制、非法访问者检测,以及关闭的时间间隔等措施,对网络服务器进行多方位的安全控制。

### 6) 网络监控和锁定控制

在网络系统中,通常服务器自动记录用户对网络资源的访问,如有非法的网络访问,服务器将以图形、文字或声音等形式向网络管理员报警,以便引起警觉进行审查。对试图登入网络者,网络服务器将自动记录企图登入网络的次数,当非法访问的次数达到设定值时,就会将该用户的账户自动锁定并进行记载。

### 7) 网络端口和节点的安全控制

网络中服务器的端口常用自动回复器、静默调制解调器等安全设施进行保护,并以加密的形式来识别节点的身份。自动回复器主要用于防范假冒合法用户;静默调制解调器用于防范黑客利用自动拨号程序进行网络攻击。还应经常对服务器端和用户端进行安全控制,如通过验证器检测用户真实身份,然后,用户端和服务器再进行相互验证。

## 7.3 网络空间作战防御的响应手段

网络空间作战防御的响应手段是指网络空间遭遇进攻或入侵时所采取的行动和措施，如各种防护方案、安全设施、策略规定。其目的是将事件造成的损失降到最低。处理方式包括事前监测、事中处理和事后的灾难恢复。处理过程分为准备、确认、封锁、根除、恢复、跟踪六个阶段。响应系统目前有三类：报警响应系统、手工响应系统和自动响应系统。响应手段主要有欺骗类攻击的防御、拒绝服务攻击的防御、口令攻击的防御、缓冲区溢出的防御、Web 攻击的防御和数据恢复技术手段，下面逐一进行介绍。

### 7.3.1 欺骗类攻击的防御

#### 1. ARP 欺骗的防御

(1) VLAN 和交换机端口绑定。通过交换机端口绑定与划分 VLAN 可以有效地防范 ARP 的欺骗。具体做法就是，根据使用的网络情况来对网络进行 VLAN 的划分，当管理员发现有非法用户在恶意利用 ARP 欺骗攻击网络，或因合法用户受 ARP 病毒影响而感染网络时，网络管理员可以利用技术手段首先查找到该用户所在的交换机端口，然后将该端口划分一个单独的 VLAN 将该用户与其他用户进行物理隔离，以避免其他用户受影响。另外，在网络设备中，大部分的网管交换机具有 MAC 地址互相学习的特殊功能，在相互学习完成之后，交换机就会自动关闭这个特殊的功能，然后把对应的 MAC 地址与相应的端口进行绑定，如此一来，从硬件设备方面就有效地避免了 ARP 攻击对自身地址的篡改。

(2) 使用 ARP 防护软件。市场上我们可以发现各种各样的 ARP 类的防护软件。在网络中，使用 ARP 类的防护软件不仅可以有效地检测出 ARP 攻击，也能够广播正确的 ARP 信息，使得网上的主机能够进行正常的网络通信。使用 ARP 类的防护软件虽然在一定的程度上减少了 ARP 攻击，但是在同一个局域网中，不能同时解决多个主机的 ARP 欺骗。因此，最好的防护方法是用户在使用电脑时要提高网络安全意识，及时为系统进行打补丁；其次，为系统设置较为复杂的使用密码；最后，使用防火墙等。现在关于 ARP 的防护软件比较多，有 ARP 保护神、Anti ARP Sniffer 等。

(3) 将病毒源机器及时处理。及时发现正在进行 ARP 欺骗的主机并将其隔离。一旦发现病毒源机器，应立即切断该机器的网络连接，并用多种杀毒软件全面查杀病毒后方可连接网络，最好是重装操作系统。要安装杀毒软件和防火墙，及时升级病毒库和防火墙数据库，定期对机器进行病毒扫描，要设置密码和账号。

(4) 在交换机或路由器上将 IP 地址与 MAC 地址绑定。启用 ARP 检查, 以过滤伪造源 MAC 地址的 ARP 攻击, 这样可以防止交换机或路由器受到 ARP 攻击。通过 MAC 地址绑定, 使网络中每一台计算机的 IP 地址与硬件地址一一对应, 不可更改。

(5) 使用静态 ARP 缓存, 用手工方法更新缓存中的记录, 使 ARP 欺骗无法进行。

(6) 使用 ARP 服务器, 通过该服务器查找自己的 ARP 转换表来响应其他机器的 ARP 广播。确保这台 ARP 服务器不被攻击。

(7) 采用路由器划分子网, 在路由器的 ARP 高速缓存中放置所有受托主机的永久条目, 也可以减少并防止 ARP 欺骗, 但路由器在寻径中同样存在安全漏洞。

## 2. 域名系统 (DNS) 欺骗的防御

DNS 欺骗主要存在两个局限性: 攻击者不能替换缓存中已经存在的记录; DNS 服务器存在缓存刷新时间问题。在侦测到网络中可能有 DNS 欺骗攻击后, 应采用下列防范措施。

(1) 对 DNS 数据包进行监测。可以通过监测 DNS 响应包, 遵循相应的原则和模型算法对这真实的数据包和攻击数据包两种响应包进行分辨, 从而避免虚假数据包的攻击。

(2) 在客户端直接使用 IP 地址访问重要的站点。这样至少可以避开 DNS 欺骗攻击。还应该做好 DNS 服务器升级 DNS 软件, 合理限定 DNS 服务器进行响应的 IP 地址区间, 关闭 DNS 服务器的递归查询项目等。

(3) 对 DNS 服务器和客户端的数据流进行加密。服务器端可以使用安全外壳 (SSH, Secure Shell) 加密协议, 客户端使用良好隐私 (PGP, Pretty Good Privacy) 软件实施数据加密。

(4) 进行 IP 地址和 MAC 地址的绑定。

(5) 优化 DNS 服务器的相关项目设置。常见的工作有以下几种: ①对不同的子网使用物理上分开的域名服务器, 从而获得 DNS 功能的冗余。②将外部和内部域名服务器从物理上分离开并使用 Forwarders 转发器。③采用技术措施限制 DNS 动态更新。④限制区域传输范围: 限制域名服务器做出响应的地址, 限制域名服务器做出响应的递归请求地址, 限制发出请求的地址。⑤利用事务签名对区域传送和区域更新进行数字签名。⑥隐藏服务器上的 Bind 版本。⑦删除运行在 DNS 服务器上的不必要的服务。⑧在网络外围和 DNS 服务器上使用防火墙, 将访问限制在那些 DNS 功能需要的端口上。⑨使用最新版本 DNS 服务器软件并及时安装补丁。⑩关闭 DNS 服务器的递归功能: DNS 服务器利用缓存中的记录信息回答查询请求, 或者 DNS 服务器通过查询其他服务器获得查询信息并将它发送给客户机, 这两种查询方式称为递归查询, 这种查询方式容易导致 DNS 欺骗。⑪采用分层的 DNS 体系结构。

## 3. IP 欺骗的防御

IP 欺骗的防范, 一方面需要目标设备采取更强有力的认证措施, 另一方面采用健壮的交互协议以提高伪装源 IP 的门槛。根据 IP 电子欺骗的特点, 提出下列综合预防策略。

(1) 监测网上数据包。通过对网络上的数据包进行监控，及时发现 IP 欺骗攻击的前兆。

(2) 对照检查本地主机之间的日志是否对应。由于大部分 IP 欺骗攻击是由攻击主机来模拟信任主机，所以通过在相互设置信任关系的主机之间，对照检查日志就可以发现 TCP 连接是否被伪造。

(3) 使用加密法并进行防火墙阻断。阻止 IP 欺骗的一个明显的方法就是在通信时要求加密传输和验证。

(4) 禁止基于 IP 地址的信任关系。IP 欺骗的原理是冒充被信任主机的 IP 地址，这种信任关系是建立在基于 IP 地址的验证上，如果禁止基于 IP 地址的信任关系、不允许 R\* 类远程调用命令的使用、删除。使所有的用户通过其他远程通信手段，如 Telnet 等进行远程访问，可彻底地防止基于 IP 地址的欺骗。更进一步，建立存取权限 ACL 来防止网络中的用户仿冒其他网络的 IP 地址。

(5) 入口过滤。大多数路由器有内置的欺骗过滤器。过滤器的最基本形式是，不允许任何从外面进入网络的数据包使用单位的内部网络地址作为源地址。因此，如果一个来自外网的数据包，声称来源于本单位的网络内部，就可以非常肯定它是假冒的数据包，应该丢弃它。

(6) 出口过滤。为了执行出口过滤，路由器必须检查数据包，确信源地址是来自本单位局域网的一个地址。如果不是那样，这个数据包应该被丢弃，因为这说明有人正使用假冒地址向另一个网络发起攻击。离开本单位的任何合法数据包须有一个源地址，并且它的网络部分与本单位的内部网络相匹配。

(7) 防止 IP 地址伪造。IP 地址伪造技术是进行 IP 欺骗采取的基本技术。具有伪造 IP 地址的报文可能发生在因特网上的任何区域。因此要防止 IP 地址伪造就需要在因特网的各级网络采用包过滤技术，截获这些伪造 IP 地址的报文。

(8) 使用反向路径转发。反向路径转发是从因特网收到数据包，取出源 IP 地址，然后查看该路由器的路由表中是否有该数据包的路由信息。如果路由表中没有其用于数据返回的路由信息，那么极有可能是某人伪造了该数据包，于是便把它丢弃。下面是在路由器上配置反向路径转发的方法：

```
Router(config)#ip cef
Router(config)#int serial10/0
Router(config-if)#ip verify unicast reverse-path
```

(9) 使用随机化的初始序列号。IP 欺骗攻击得以成功实现的一个很重要的因素就是，TCP/IP 的数据包序列号不是随机选择的或随机增加的。为此，可以采用分割序列号空间的办法，这样每一个连接将有自己独立的序列号空间。序列号仍然按照以前的方式增加，但是在这些序列号空间之间没有明显的关系。



## 4. 路由欺骗防御

### 1) RIP 路由欺骗的防御

RIP 路由欺骗的防范措施主要有：路由器在接受新路由前应先验证其是否可达。这可以大大降低受此类攻击的概率。但是 RIP 的有些实现并不进行验证，使一些假路由信息也能够广泛流传。由于路由信息在网上可见，随着假路由信息在网上的传播范围扩大，它被发现的可能性也在增大。所以，对于系统管理员而言，经常检查日志文件会有助于发现此类问题。对 RIP 包进行身份认证，可杜绝假冒路由器。

防止 RIP 欺骗的一种途径是停止使用 RIP 的被动工作模式，尤其是一个较大网络系统涉及多个路由器时，应限制性的使用 RIP 协议。在网络拓扑结构相对稳定一个局域网内，可以停止使用 RIP 的被动工作模式，如果需要更新路由表可采用定期检查与更新，减少被攻击的概率，也可应用其他方法来实现，如发送信任的 ICMP 报文。为保证较高的安全性，RIP 协议被动参与者必须采用一些认证方法来接收值得信任的 RIP 报文，简单办法就是，可以在主机或路由器每次启动时查阅一个配置文件，确定哪些是具有值得信任 RIP 信息的 IP 地址，从而减少欺骗的发生。当然也可以使用其他路由协议代替 RIP，如链路状态路由协议，开放 SPF 协议，后者更为先进、有效。

### 2) IP 源路由欺骗的防御

防范 IP 源路由欺骗的好方法主要有：配置好路由器，使它抛弃那些由外部网进来的、声称是内部主机的报文；关闭主机和路由器上的源路由功能。

### 3) 基于 ICMP 的路由欺骗的防御

避免 ICMP 重定向欺骗的最简单方法是将主机配置成不处理 ICMP 重定向消息。这样数据包仍进行发送，如同该 ICMP 没有作用一样，从而可以避免简单的路由欺骗技术（发送非法 ICMP 重定向消息）。

另一种方法是，确保主机 ARP 缓存中保存所有合法路由器的永久地址项，并验证所有 ICMP 重定向消息，由此可以有效地防止伪路由器进行的路由欺骗。检查 ICMP 重定向消息是否来自当前正在使用的路由器，需要检查重定向消息发送者的 IP 地址，并校验该 IP 地址对应的硬件地址与 ARP 缓存中合法路由器的永久项是否匹配。

### 4) 基于 RIP 的路由欺骗的防御

要防止 RIP 路由欺骗的途径是停止路由器被动参与 RIP，并且与其他路由器之间改用其他路由协议，如链路状态协议，但路由器仍主动参与 RIP，每隔 30 秒为主机广播路由信息。这样，恶意的 RIP 广播报文就不会波及整个组织的网络。但是，单独的主机由于被动参与 RIP，所以仍然很容易遭受 RIP 欺骗。

实际上，问题在于对 RIP 信息源的信任。要保证安全性，RIP 协议的被动参与者必须只接受可信的信息源。因此，可以配置成只接受可信路由器的 RIP。

## 5. 万维网（WWW）欺骗的防御

对于 WWW 欺骗技术的防范，首先，必须管理好 Cookie，对其设定级别加密。其次，用户要对自己的信息进行保护，定期对以往的记录进行清除，尽量不要在浏览器中自动保存密码信息。最后，对 Java 程序和 ActiveX 控件进行阻止。此外，还要对访问过的网页及时进行清除。

## 6. 电子邮件欺骗的防御

作为互联网用户，必须时刻树立风险意识，不要随意打开一个不可信任的邮件。

作为邮件接收者来说，用户需要合理配置邮件客户端，使每次总能显示出完整的电子邮件地址，而不是仅仅显示别名，完整的电子邮件地址能提供一些迹象表明正在发生一些不平常的事情。用户应该注意检验发件人字段，不要被相似的发信地址所蒙蔽。

作为邮件发送者来说，如果使用 Foxmail 或者 Outlook 之类的邮件客户端，必须保护好这些邮件客户端，防止他人对客户端的设置进行修改。

作为邮件服务器提供方来说，采用 SMTP 身份验证机制。原来使用 SMTP 协议发送邮件的时候并不需要任何验证，身份欺骗极易实现。现在将入网点（POP）协议收取邮件需要用户名/密码验证的思想移至 SMTP 协议，发送邮件也需要类似的验证。绝大多数邮件服务提供商都是采用这种做法，通常是使用与接收邮件相同的用户名和密码来发送邮件。采用这种方法后，虽然 SMTP 协议安全性问题仍然无法从根本上得到解决，但电子邮件欺骗已经变得不像过去那么容易了。

防范的另一方法就是 PGP 加密。可能的解决方法就是使用公钥加密，其中应用最广泛的是 PGP 邮件加密。PGP 是一个可以让电子邮件拥有保密功能的程序。由此可以将邮件加密，一旦加密后，邮件看起来是一堆无意义的乱码。PGP 提供了极强的保护功能，即使最先进的解码分析技术也无法解读加密后的文字。举例来说，当要传送一封保密信或档案给某人时，必须先取得那人的公钥，然后利用这个公钥将信件加密。当某人收到加密的信件后，他必须利用相应的私钥来解密。因此，除非其他人拥有收信者的私钥，否则无法解开发信人所加密的信件。同时，收信人在使用私钥解密时，还必须输入通行码，这样又对加密后的邮件多了一层保护。

### 7.3.2 拒绝服务攻击的防御

拒绝服务（DoS）攻击防御的困难之处在于：

- （1）不容易定位攻击者的位置。互联网上绝大多数网络都不限制源地址，因此伪造源地址非常容易；很难追踪找到攻击控制端的位置；各种反射式攻击，无法定位源攻击者。
- （2）完全阻止是不可能的，但是适当的防范工作可以减少被攻击的机会。

DoS 攻击手段多、变化快、实施简单、隐蔽性强，具有较大的危害性。如何有效地防御 DoS 攻击是一项系统化的工作，也是有待进一步研究的问题。目前针对各种现有的 DoS 攻击有许多防御或缓解策略，如果能够有效组合起来，可在一定程度上防范 DoS 攻击。

## 1. DoS 的防御方法

### 1) 有效完善的设计

一个站点越完善，它的状况会越好。若有一个运行关键任务的 Web 站点，用户必须连接互联网，但是与路由器之间只有一条单一的连接，服务器运行在一台单一的计算机上，这样的设计就不是完善的。这种情况下，攻击者对路由器或服务器进行 DoS 攻击，使运行关键任务的应用程序被迫离线。在理想情况下，不仅要有多条与互联网的连接，最好有不同地理区域的连接。服务位置越分散，IP 地址越分散，攻击同时寻找与定位所有计算机的难度就越大。

### 2) 充足的网络带宽保证，并限制端口带宽

网络带宽直接决定了能抗受攻击的能力，假若仅仅有 10M 带宽的话，无论采取什么措施都很难对抗当今的 SYN Flood 攻击，至少要选择 100M 的共享带宽，最好的当然是挂在 1000M 的主干线上。但需要注意的是，主机上的网卡是 1000M 的并不意味着它的网络带宽就是千兆的，若把它接在 100M 的交换机上，它的实际带宽不会超过 100M，再就是接在 100M 的带宽上也不等于就有了百兆的带宽，因为网络服务商很可能会在交换机上限制实际带宽为 10M，这点一定要搞清楚。

当 DoS 攻击发生时，针对单个协议的攻击会损耗带宽，以致拒绝合法用户的服务。例如，如果攻击者向端口 25 发送洪水般的数据，攻击者会消耗掉所有带宽，所以试图连接端口 80 的用户被拒绝服务。一种防范方法是限制基于协议的带宽。例如，端口 25 只能使用 25% 的带宽，端口 80 只能使用 50% 的带宽。

### 3) 升级

升级操作系统以及各种网络应用程序，安全设置服务器及网络设备，避免由于软件缺陷或用户设置不当造成的拒绝服务攻击。

升级网络带宽，抵御带宽耗尽型攻击。升级网络设备，使网络设备不至于在受到攻击时，成为瓶颈。升级服务器，提高服务器处理性能。部署专用抗拒绝服务攻击设备，以及 IDS。

升级主机服务器硬件。在有网络带宽保证的前提下，请尽量提升硬件配置，要有效对抗每秒 10 万个 SYN 攻击包，服务器的配置至少应该为：P42.4G/DDR512M/SCSI-HD，起关键作用的主要是 CPU 和内存，内存一定要选择双倍速率（DDR，Double Data Rate）的高速内存，硬盘要尽量选择小型计算机系统接口（SCSI，Small Computer System Interface）的，别只贪图电子集成驱动器（IDE，Integrated Drive Electronics）价格不贵量还足的便宜，否则会付出高昂的性能代价，再就是网卡一定要选用名牌厂家的。

采用高性能的网络设备。首先要保证网络设备不能成为瓶颈，因此选择路由器、交换机、硬件防火墙等设备的时候要尽量选用知名度高、口碑好的产品。再就是假如和网络提供商有特殊关系或协议的话就更好了，当大量攻击发生的时候请他们在网络节点处做一下流量限制，这对对抗某些种类的 DoS 攻击是非常有效的。

及时给系统安装补丁。当新的 DoS 攻击出现并攻击计算机时，厂商一般会很快确定问题并发布补丁。如果一个单位关注最新的补丁，同时及时安装，这样被 DoS 攻击的机会就会减少。记住：这些措施并不能阻止 DoS 攻击耗尽公司的资源。还有在安装补丁之前，先要对其进行测试。即使厂商声明它可以弥补 DoS 漏洞，这并不意味着不会产生新的问题。

#### 4) 优化设置以达到防御的目的

优化路由器设置，关闭不需要的服务，保障路由器自身安全。关闭 ICMP 服务，尤其不允许出栈 ICMP “不可到达” 消息，通常正常使用时，我们并不需要 ICMP 服务。另外，禁止不需要使用的 UDP 包通过。启用单一地址逆向转发功能，可以防范来自内部的伪造 IP 的攻击。设置 TCP 拦截，防范 SYN Flood 攻击。使用基于内容的访问控制，通过监视半连接数量和产生频率来防止洪水攻击。使用 QoS 的各种特征来防范拒绝服务攻击，但需要注意的是，不同的 QoS 策略对于不同的拒绝服务攻击效果是有差别的。过滤所有 RFC1918 私有 IP 地址。

路由器作为整个互联网的组网设备，可惜的是，大部分厂家的路由器都没有直接针对 DoS 的防御功能，Cisco 路由器添加了连接监控功能，性能一般。但是，可以通过使用路由器一些访问控制和 QoS 设置功能来达到防御 DoS 的目的。

(1) 启用反向路径转发 (RPF, Reverse Path Forwarding) 机制。在使用 Cisco 特快交换的路由器上，RPF 规定路由器收到任何一个数据包，首先检查返回该数据包的源 IP 的路由是不是从接收到该数据包的接口出去，如果是，则转发数据包，如果不是则丢弃该数据包，这样可以有效地限制源 IP 是不可达 IP 地址的数据包的转发。

(2) 使用控制接入速率 (CAR, Control Access Rate) 功能限制流速率。如果管理员发现网络中存在 DoS 攻击，并通过 sniffer 或其他手段得知发起 DoS 攻击的数据流的类型，然后可给该数据流设置一个上限带宽，这样超过了该上限的攻击流量就被丢弃，可以保证网络带宽不被占满。

(3) 过滤流量。中小单位的网络管理员可以在边界路由器上使用访问控制列表过滤掉 RFC 1918 中规定的私有 IP 的数据流量；另外，还可以设置只允许本单位内部 IP 发起的数据流通过路由器，尽量确保数据流的准确性。

#### 5) 优化服务器或应用程序本身

比如 Windows 2000 和 Windows Server 2003 操作系统，本身就具备一定的抵抗拒绝服务攻击的能力，只是默认状态下没有开启，开启的话自身就可以抵御 10 000 个 SYN 攻击包，若没有开启仅能抵御数百个。另外，比如 Apache 服务器默认情况下只允许 200 个活动连接，MySQL 默认只允许 50 个连接，通过重新编译，可以提高连接数值，来防止连接

耗尽型拒绝服务攻击。

#### 6) 运行尽可能少的服务

运行尽可能少的服务可以减少被攻击成功的机会。如果一台计算机开了 20 个端口，这就使得攻击者可以在大的范围内尝试对每个端口进行不同的攻击。相反，如果系统只开了两个端口，这就限制了攻击者攻击站点的攻击类型。另外，当运行的服务和开放的端口都很少时，管理员可以很容易地设置安全防线，因为要监听和担心的事情都很少了。

#### 7) 只允许必要的通信

这一防御机制与上一条“运行尽可能少的服务”很相似，不过它侧重于周边环境，主要是防火墙和路由器。关键是不仅要对系统实施最少权限原则，对网络也要实施最少权限原则。确保防火墙只允许必要的通信出入网络。许多单位只过滤进入通信，而对向外的通信不采取任何措施。这两种通信都应该过滤。

#### 8) 封锁敌意 IP 地址

当一个单位知道自己受到攻击时，应该马上确定发起攻击的 IP 地址，并在其外部路由器上封锁此 IP 地址。这样做的问题是，即使在外网路由器上封锁了这些 IP 地址，路由器仍然会因为数据量太多而堵塞，导致合法用户被拒绝对其他系统或网络的访问。因此，一旦单位受到攻击应立刻通知其 ISP 和上游提供商封锁敌意数据包。因为 ISP 拥有较大的带宽和多点的访问，如果他们封锁了敌意通信，仍然可以保持合法用户的通信，也可以恢复遭受攻击单位的连接。

#### 9) 尽量避免 NAT 的使用

无论是路由器还是硬件防火墙设备要尽量避免采用网络地址转换 NAT 的使用，因为采用此技术会较大降低网络通信能力，其实原因很简单，因为 NAT 需要对地址来回转换，转换过程中需要对网络包的校验和进行计算，因此浪费了很多 CPU 的时间，但有些时候必须使用 NAT，那就没有好办法了。

#### 10) 把网站做成静态页面

大量事实证明，把网站尽可能做成静态页面，不仅能大大提高抗攻击能力，而且还给黑客入侵带来不少麻烦，至少到现在为止关于 HTML 的溢出还没出现，新浪、搜狐、网易等门户网站主要都是静态页面，若你非常需要动态脚本调用，那就把它弄到另外一台单独主机去，免得遭受攻击时连累主服务器，当然，适当放一些不做数据库调用脚本还是可以的。此外，最好在需要调用数据库的脚本中拒绝使用代理访问，因为经验表明使用代理访问你网站的 80% 属于恶意行为。

## 2. 分布式拒绝服务攻击的防御

虽然还没有很好的措施来彻底解决分布式拒绝服务攻击问题，但下面有一些措施能降

低系统受到拒绝服务攻击的危害：优化网络和路由结构、保护网络及主机系统安全、安装入侵检测系统、与 ISP 服务商合作和使用扫描工具。

#### 1) 优化网络和路由结构

在理想情况下，提供的服务不仅要有多条与因特网的连接，而且最好有不同地理区域的连接。这样服务器 IP 地址越分散，攻击者定位目标的难度就越大，当问题发生时，所有的通信都可以被重新路由，可以大大降低其影响。

#### 2) 保护网络及主机系统安全

本质上，如果攻击者无法获得网络的访问权，无法攻克一台主机，他就无法在系统上安装 DDoS 服务器。要使一个系统成为服务器，首先要以某种手段攻克它。如果周边环境不会被突破，系统能够保持安全，就不会被用于攻击其他系统。对所有可能成为目标的主机都进行优化，禁止不必要的服务，这样可以减少被攻击的机会。要注意保护主机系统的安全，避免其被攻击者用作傀儡主机，充当 DDoS 的间接受害者。

#### 3) 安装入侵检测系统

能否尽可能快地探测到攻击是非常关键的。从 DDoS 的角度来看，单位越快探测到系统被入侵或服务器被用来进行攻击，该单位的网络状况越好。借助于 IDS 可以完成这一工作，有两种常用的 IDS：基于网络的和基于主机的。

(1) 基于网络的 IDS 是网络上被动的设备，负责嗅探通过给定网段的所有数据包。通过查看数据包，查找显示可能的攻击的签名并对可疑行为发出警报。

(2) 基于主机的 IDS 运行在一台独立服务器上，并经常查看审计日志查找可能的攻击信息。

正如有两种类型 IDS 一样，也有两种构建 IDS 的技术：样式匹配和不规则探测。①样式匹配技术有一个关于已知攻击特征的数据库，当它找到与给定样式相同的数据包时就发出警报；②不规则探测系统决定什么是网络的正常通信，任何不符合这一规则的通信都被标为可疑的。

可以想象，基于不规则探测的系统实现起来十分困难，因为对于一家单位是正常的通信而对于另一家单位则是不正常的。因此大多数入侵检测系统都是基于样式匹配技术的。

#### 4) 与 ISP 服务商合作

这一点非常重要。DDoS 攻击非常重要的一个特点是洪水般的网络流量，耗用了大量带宽，单凭自己管理网络，是无法对付这些攻击的。当受到攻击时，与 ISP 协商，确定发起攻击的 IP 地址，请求 ISP 实施正确的路由访问控制策略，封锁来自敌意 IP 地址的数据包，减轻网络负担，防止网络拥塞，保护带宽和内部网络。

#### 5) 使用扫描工具

由于许多单位网络安全措施都进行得很慢，他们的网络可能已经被攻克并用作了

DDoS 服务器，因此要扫描这些网络查找 DDoS 服务器并尽可能地把它们从系统中关闭删除。一些工具可做到这些，而且大多数商用的漏洞扫描程序都能检测到系统是否被用作 DDoS 服务器。

### 7.3.3 口令攻击的防御

#### 1. 口令破解防御

口令破解防范办法很简单，只要使自己的口令不在英语字典中，且不可能被别人猜测出就可以了。一个好的口令应当至少有 8 个字符长，不要用个人信息（如生日、名字等），口令中要有一些非字母字符（如数字、标点符号、控制字符等），还要好记一些，不能写在纸上或计算机的文件中。

保持口令的安全要点包括以下几点：（1）不要将口令写下来；（2）不要将口令存于计算机文件中；（3）不要选取显而易见的信息当口令；（4）不要让别人知道；（5）不要在不同系统上使用同一口令；（6）为了防止眼疾手快的人窃取口令，在输入口令时应当确定无人在身边；（7）定期更换口令，至少 6 个月要改变一次。

#### 2. 强口令的选取方法

强口令的定义差别很大，它和单位的业务类型、位置、雇员等的因素有关。强调这一点是因为会因所处的环境不同而差别很大。定义也会因技术的增强而变化。

比如说，五年前曾被认为是强口令，现在很可能就会变成弱口令。导致这种变化的主要原因就是计算机系统比五年前的计算机系统更快和更便宜。五年前用最快的计算机破解要花几年的时间的口令，现在只要不到 1 小时就解开了。

什么才是强口令呢？基于目前的技术，强口令必须具备以下的特征：（1）每 45 天换一次；（2）口令至少包含 10 个字符；（3）必须包含字母、数字、特殊的符号；（4）字母、数字、特殊符号必须混合起来，而不是添加在尾部；（5）不能包含词典单词；（6）不能重复使用以前的五个口令；（7）一定次数登录失败后，口令在一段时间封闭。

提议用户用句子而不是用单词作为口令。这就要选取一个容易记忆、不含词典中的单词、含有数字和特殊字符的口令。如使用每个单词的第一个字母作为口令。比如说，如果口令“Wlsmtls#¥%\*5t”，如果就这样记的话是非常困难的，但是如果你记住这句话“When I stub my toe I say “#¥%\*” 5 times”（我的脚趾头被绊时我说了 5 次“#¥%\*”），这样的口令可能就会被记住了。简单地取每个单词的首字母，就组成了一个口令。

#### 3. 保护口令的方法

强口令的选取是从用户的角度来说的，那么，对于系统来说，口令的安全又是如何得

到保障的呢？系统中存的任何口令都必须受到保护，防止未授权泄露、修改和删除。

未授权泄露在口令安全中占有重要的地位。如果攻击者能得到口令的副本，则读取口令后，他就能获得系统访问权。这就是为什么强调用户不能将口令写下或透露给同事的原因。如果攻击者能得到口令的副本，他会变成合法用户，所做的一切最后都会追踪到那个合法用户身上。

未授权修改也很重要，因为即使攻击者无法读到口令，但是可用他所知道的单词修改口令，这样你的口令变成了攻击者知道的值，他不需要知道实际口令就能做到这一点。这在各种操作系统中成了主要问题。

未授权的删除也很重要，因为攻击者删除账号，或者导致拒绝服务攻击，或者用他知道的口令重新创建该账号。比方说，攻击者在周末闯入了系统并删除了所有的用户账号，这就产生了一次拒绝服务攻击，因为星期一所有人都无法登录系统，被系统拒绝访问。

要保护口令不被未授权泄露、修改和删除，口令就不能按纯文本方式存放在系统内，如果系统中存放有包含所有口令的文本文件，很容易被某些人读取并获得所有人的口令。

保护口令的一个很重要的方法就是加密。加密能隐藏原始文本，所以如果有人得到了加密口令，也无法确定原始口令。密码学最基本的形式就是把明文隐藏为密文，目的是让它不可读。在这里，明文是原始消息或可读口令，密文是加密的或不可读的版本。

#### 4. 一次性口令技术

仅从字面上理解，一次性口令技术好像要求用户每次使用时都要输入一个新的口令。但事实正相反，用户所使用的仍然是同一个口令。一次性口令技术采用的是挑战-响应机制。一次性口令的工作原理可描述如下：

(1) 首先在用户和远程服务器之间建立一个秘密，该秘密在此被称为“通行短语”，相当于传统口令技术当中的“口令”。同时，它们之间还具备一种相同的“计算器”，该计算器实际上是某种算法的硬件或软件实现，它的作用是生成一次性口令。

(2) 当用户向服务器发出连接请求时，服务器向用户提示输入种子值。种子值(seed)是分配给用户的在系统内具有唯一性的一个数值，也就是说，一个种子对应一个用户，同时它是非保密的；可以把种子值形象地理解为用户名。

(3) 服务器收到用户名之后，给用户回发一个迭代值作为“挑战”。迭代值(iteration)是服务器临时产生的一个数值，与通行短语和种子值不同的是：它总是不断变化的。可以把迭代值形象地理解为一个随机数。

(4) 用户接到挑战后，将种子值，迭代值和通行短语输入到“计算器”中进行计算，并把结果作为回答返回服务器。

(5) 服务器暂存从用户那里收到的回答。因为它也知道用户的通行短语，所以它能计算出用户正确的回答，通过比较就可以核实用户的确切身份。

以上的一次性口令过程可用图 7-15 表示。

我们可以看出，用户通过网络传给服务器的口令是种子值、迭代值和通行短语在计算器作用下的计算结果，用户本身的通行短语并没有在网上传播。



只要计算器足够复杂，就很难从中提取出原始的通行短语，从而有效地抵御了网络监听攻击。又因为迭代值总是不断变化的，比如每当身份认证成功时，将用户的迭代值自动减 1，这使得下一次用户登录时使用鉴别信息与上次不同（一次性口令技术由此得名），从而有效地阻止了重放攻击。

总之，与传统口令技术的单因子（口令）鉴别不同，一次性口令技术是一种多因子（种子值、迭代值和通行短语）鉴别技术，其中引入的不确定因子使得它更为安全。

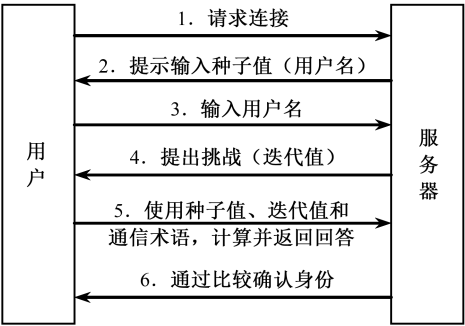


图 7-15 一次性口令过程

5. 生物技术口令

随着生物技术和计算机技术的发展，人们发现人的许多生理特征如指纹、掌纹、面孔、声音、虹膜、视网膜等都具有唯一性和稳定性，每个人的这些特征都与别人不同，且终身不变，也不可能复制。这使得通过识别用户的这些生理特征来认证用户身份的安全性远高于基于口令的认证方式。

人们发展了指纹识别、视网膜识别、发音识别等多种生物识别技术，其中以指纹识别技术发展得最为火热。指纹自动柜员机、指纹电子商务、指纹网络管理、指纹加密文件、指纹财务管理、指纹手持终端等，就连现在许多笔记本上都使用了指纹识别器。

由于计算机在处理指纹时，要将生理特征转化为数据，只涉及了指纹的一些有限信息，而且对比算法不能保证 100%精确匹配，因此，在应用系统的设计中，要充分考虑识别率（包括漏判和误判）的问题。

7.3.4 缓冲区溢出的防御

缓冲区溢出是一种非常危险且极为常见的漏洞。在过去的十年中，以缓冲区溢出为类型的安全漏洞是最为常见的一种形式。更为严重的是，缓冲区溢出漏洞占了远程网络攻击的绝大多数，这种攻击可以使得一个匿名的互联网用户有机会获得一台主机的部分或全部的控制权。

缓冲区溢出的真正原因在于某些编程语言缺乏类型安全，程序缺少边界检查。一方面是源于编程语言和库函数本身的弱点，如 C 语言中对数组和指针引用不自动进行边界检查，一些字符串处理函数如 strcpy、sprintf 等存在着严重的安全问题。另一方面是程序员进行程序编写时，由于经验不足或粗心大意，没有进行或忽略了边界检查，使得缓冲区溢出漏洞几乎无处不在，为缓冲区溢出攻击留下了隐患。

这样要么放弃使用这类语言中的不安全类型，放弃不安全的类型就等于放弃这类语言的精华；要么使用其他的类型安全语言，如 Java 等，而放弃 C/C++ 语言等这些高效易用的编程语言对于大部分程序员又是不能接受的，所以只能采取其他的防护措施。

首先，可以考虑在一般的攻击防护产品中加入针对缓冲区溢出攻击的防护功能，如防火墙和 IDS 等。可以从两个方面着手：一是可以提取用于攻击的 shellcode 的普遍特征作为攻击特征，过滤掉这样的数据包或触发报警。二是对特定的服务限定请求数据的值的范围，比如，某一服务要求请求数据为可打印字符串，如果发现对这一服务的请求存在不可打印字符则认为发生攻击。

其次，通过分析缓冲区溢出攻击的原理，可以发现缓冲区溢出能够成功的条件：编译器本身或库函数没有对数组类型的数据结构做严格的边界检查，这是溢出的首要原因；返回地址放在堆栈的底部，使得通过溢出可以覆盖返回地址；堆栈的属性一般是可执行的，使得恶意代码得以执行。

### 1. 源码级保护方法

源码级保护有 3 种方法：避免源码中的相关 bug、源码中溢出 bug 的查找和数组边界检查编译器。

#### 1) 避免源码中的相关 bug

防患于未然。在软件开发过程中，对涉及缓冲区的操作，做严格的边界检查，从代码编写层防止缓冲区溢出。C 语言是其中最具代表性的一种，由于只追求性能的传统认识，它具有容易出错的倾向，有许多字符串处理函数存在未检查输入参数长度和边界问题、字符串以 0 结尾而不是用下标管理等。对使用 C 语言的开发人员来说，放弃这种高效易用的编程语言是不能接受的，因此，只能要求程序员提高自身编程水平，在编写程序时尽量避免有错误倾向的代码出现。不过，保证代码的正确性和安全性是一个非常复杂的问题，这也使开发人员的工作效率大大降低。在现代的程序开发中，应用程序往往十分庞大，加之程序员的经验有限，要想彻底避免此类问题，在实际应用中往往是很难做到的。使用 C 库函数时程序员要注意自行检查边界，或者尽可能使用其对应的替代函数。

#### 2) 源码中溢出 bug 的查找

人们尝试开发一些工具，对程序溢出漏洞的代码进行审计。也就是利用工具对源码中可能存在溢出 bug 的部分代码进行分析以发现 bug。最简单的方法就是搜索源码中容易产生漏洞的库函数调用，如典型的 strcpy 和 sprintf 这两个函数调用，它们都没有检查输入参数的长度。如利用 grep 来查找和搜索。这种方法虽然可以提高查找的效率，但是它需要较多的专业知识，要求安全审计人员对语言本身非常熟悉。同时由于 grep 只是简单地对字符串进行匹配，只能发现众多问题中的很小的一部分，通常只能作为辅助工具使用。

一些组织和实验室开发了一些高级的查错工具，如 Fault Injection、ITS4 等。ITS4 是针对 C/C++ 设计的静态分析工具，可以在 Windows、UNIX/Linux 环境下使用。它通过

扫描源代码、对源代码执行模式匹配来进行工作，对可能危险的模式（如特定的函数调用）进行提取和分析，确定危险的程度，对危险的函数调用提供问题的说明和如何修复源代码的建议。

### 3) 数组边界检查编译器

数组边界检查编译器，将边界检查转换成安全策略中的推理规则，由符号解释器和定理证明器来扫描解释目标代码指令，以判定目标代码是否符合指定的安全策略。

## 2. 运行期保护方法

运行期保护方法主要研究如何在程序运行的过程中发现或阻止缓冲区溢出攻击。这种方法具有简洁、方便的特点，而且对相关知识要求不高，因而更为实用。目前，动态保护研究的主要方面是数组边界检查和如何保证返回指针的完整性。

只要数组不被溢出，溢出攻击也就无从谈起。数组边界检查就是检查数组实际长度是否超过了分配的长度。如果超过，立即进行相应的处理，如舍去超出分配长度的部分。

### 1) 插入目标代码进行数组边界检查

为了实现数组边界检查，对所有的数组的读写操作都应当被检查以确保对数组的操作在正确的范围内。最直接的方法是检查所有的数组操作，但是通常可以采用一些优化的技术来减少检查的次数。

目前的检查方法有 Compaq C 编译器、Jones & Kelly 的 C 数组边界检查、Purify 的存储器存取检查和类型-安全语言。

(1) Compaq C 编译器。Compaq 公司为 Alpha CPU 开发的 C 编译器支持有限度的边界检查（使用 `-check_bounds` 参数）。这些限制只有显示的数组引用才被检查，比如“`a[3]`”会被检查，而“`*(a+3)`”则不会。由于所有的 C 数组在传送的时候是指针传递的，所以传递给函数的数组不会被检查。带有危险性的库函数如 `strcpy` 不会在编译的时候进行边界检查，即便是指定了边界检查。

由于在 C 语言中利用指针进行数组操作和传递是如此的频繁，因此这种局限性是非常严重的。通常这种边界检查用于程序的查错，而且不能保证程序中没有缓冲区溢出的漏洞。

(2) Jones & Kelly 的 C 数组边界检查。Richard Jones 和 Paul Kelly 开发了一个 gcc 的补丁，用来实现对 C 程序完全的数组边界检查。由于没有改变指针的含义，所以被编译的程序和其他的 gcc 模块具有很好的兼容性。更进一步的是，他们由此从没有指针的表达式中导出了一个“基”指针，然后通过检查这个基指针来侦测表达式的结果是否在允许的范围之内。

当然，这样付出的性能上的代价是巨大的：对于一个频繁使用指针的程序如向量乘法，将由于指针的频繁使用而使速度只能达到原来的三十分之一。这个编译器目前还很成熟，而且一些复杂的程序还不能在这个上面编译。

(3) Purify 的存储器存取检查。Purify 是 C 程序调试时查看存储器使用的工具而不是

专用的安全工具。Purify 使用“目标代码插入”技术来检查所有的存储器存取。通过用 Purify 连接工具连接，可执行代码在执行的时候的性能只有原来的三十五分之一。

(4) 类型-安全语言。所有的缓冲区溢出漏洞都源于语言缺乏类型安全。如果只有类型安全的操作才可以被允许执行，这样就不可能出现对变量的强制操作。如果作为新手，可以推荐使用具有类型-安全语言，如 Java 和 C#。

但是，作为 Java 执行平台的 Java 虚拟机是 C 程序，因此通过攻击 Java 虚拟机 (JVM, Java Virtual Machine) 的一条途径可以使 JVM 的缓冲区溢出。

## 2) 返回指针的完整性检查

程序指针完整性检查和边界检查的思路不同。它不是防止程序指针被改变，而是在程序指针被引用之前检测它是否被改变。因此，即便一个攻击者成功地改变了程序的指针，系统会事先检测到指针的改变，而废弃这个指针。

返回指针的完整性检查主要采用了堆栈监测、StackGuard、StackShield 等手段。

(1) 堆栈监测。堆栈监测是一种提供程序指针完整性检查的编译器技术，通过检查函数活动记录中的返回地址来实现。它在每个函数中，加入了函数建立和销毁的代码，加入的函数建立代码实际上在堆栈中的函数返回地址前面加了一些附加的字节，而在函数返回时，首先检查这个附加的字节是否被改动过，若发生过缓冲区溢出，那么就很容易在函数返回前被检测到。

(2) StackGuard。StackGuard 是标准 GNU 的 C 编译器 gcc 的一个修改版。它通过在函数返回地址之前插入一个“守卫”值 (canary 值)，在函数返回前检查 canary 值是否被修改，来保证返回地址的完整性。StackGuard 作为 gcc 的一个补丁，修改了函数建立和销毁部分的代码，由这些代码来完成 canary 值插入和 canary 值检查工作。

(3) StackShield。StackShield 采用的方法略有不同。它另外创建一个堆栈用来储存函数返回地址的一份拷贝。在受保护的函数的开头和结尾分别增加一段代码，开头处的代码用来将函数返回地址拷贝到一个特殊的表中，而结尾处的代码用来将返回地址从表中拷贝回堆栈。因此即使返回地址被覆盖，函数执行流程也不会改变，将总是正确返回到调用函数中。

但由于没有比较堆栈中的返回地址与保存的地址是否相同，因此并不能得知是否发生了堆栈溢出。在最新的版本中已经增加了一些新的保护措施，当调用一个地址在非文本段内的函数指针时，将终止函数的执行。

## 3. 阻止攻击代码执行

当程序的执行流程已经被重定向到攻击者的恶意代码时，前述的防护措施都已经失效。这时仍然可以采取一定的措施阻止攻击的形成——阻止攻击代码执行。可以采用非执行缓冲区技术，即通过设置缓冲区地址空间的属性为不可执行，使得攻击代码不能执行，从而避免攻击，这种技术被称为非执行的缓冲区技术。

设置缓冲区最初的目的是用来存放数据而不是可执行代码，因此这样做本不应当带来

兼容性的问题。但是近来的 UNIX 和 MS Windows 系统为了便捷地实现某些功能，往往允许在数据段中放入可执行代码，为了保证程序的兼容性，不可能使程序所有的数据段都不可执行。不过，可以设定堆栈数据段不可执行，因为几乎没有任何程序会在堆栈中存放代码，这样就可以最大限度地保证程序的兼容性。

#### 4. 加强系统保护

软件开发中的安全编程只能尽量减少缓冲区溢出的可能，并不能完全地消除它的存在，管理员不可避免的还会面对缓冲区溢出攻击的威胁。因此在系统管理阶段仍然应该尽可能安全地配置其系统及系统提供的服务，以减少缓冲区溢出的威胁。

这里以 Linux 系统的配置为例提出安全配置的主要原则：保护系统信息、关闭不需要的服务、最小权限原则、使用系统的堆栈补丁、检查系统漏洞，及时为软件打上安全补丁。

##### 1) 保护系统信息

攻击者需要系统信息才能确定缓冲区溢出漏洞所在，隐藏系统信息可以获得对系统最低限度的保护。方法有：①使系统本地登录时不显示 Linux 发行版本名字、版本号、内核版本和服务名称；②不显示系统远程登录提示信息；③使系统对 Ping 没有反应。

##### 2) 关闭不需要的服务

不必要的对外服务往往会提供攻击者所需的漏洞，可采用下列方法：①禁止提供 finger 服务；②处理“inetd.conf”文件，对于在网络环境中的 Linux 系统，首要的就是确定需要被监听的网络端口，为每个端口启动相应服务，并卸载不必要的服务；③修改系统的“rc”启动脚本，仅仅启动系统必需的服务；④处理“services”文件，使其不可被用户修改。

##### 3) 最小权限原则

缓冲区溢出漏洞的目标往往是 setuid/setgid 等具有特殊权限的程序。这使得权限中包含“s”位的程序往往成为系统不安全的主要因素。方法主要有：①取消普通用户的控制台访问权限；②减少特权程序的使用。

如果文件的权限位中出现“s”，则这些文件的 SUID（-rwsr-xr-x）或 SGID（r-xr-sr-x）位被设定了。因为这些程序给执行它的用户一些特权，可以被攻击者恶意利用来提示自身权限。因此，如果不需要用到这些特权，最好把这些程序的“s”位移去。可以用“chmod a-s<文件名>”移去相应文件的“s”位。

##### 4) 使用系统的堆栈补丁

在安全编程中使用不可执行堆栈有一些好处，但那是针对开发者的要求。可是，系统管理员所使用的程序或软件往往不带有这样的配置，因此应该尽量去主动获得并安装操作系统提供商所发布的系统堆栈补丁。

### 5) 检查系统漏洞，及时为软件打上安全补丁

这也是最为常见的做法，管理员应该经常性的关注安全消息，尽快地获得软件安全漏洞报告，并采取相应的措施，如及时为软件打上补丁。这对弥补缓冲区溢出漏洞之外的其他安全缺陷也是很重要的。

## 7.3.5 Web 攻击的防御

### 1. Web 的安全防护技术

#### 1) Web 客户端的安全防护

Web 客户端的防护措施，重点对 Web 程序组件的安全进行防护，严格限制从网络上任意下载程序并在本地执行。可以在浏览器进行设置，如 Microsoft Internet Explorer 的 Internet 选项的高级窗口中将 Java 相关选项关闭。在安全窗口中选择自定义级别，将 ActiveX 组件的相关选项禁用。在隐私窗口中根据需要选择 Cookie 的级别，也可以根据需要删除 c:\windows\cookie 下的所有 Cookie 相关文件。

#### 2) 通信信道的安全防护

通信信道的防护措施，可在安全性要求较高的环境中，利用基于 SSL 的 HTTPS (HTTP over SSL) 替代 HTTP。利用安全套接层协议 SSL 保证安全传输文件，SSL 通过在客户端浏览器软件和 Web 服务器之间建立一条安全通信信道，实现信息在因特网中传送的保密性和完整性。但 SSL 会造成 Web 服务器性能下降。

#### 3) Web 服务器端的安全防护

限制在 Web 服务器中账户数量，对在 Web 服务器上建立的账户，在口令长度及定期更改方面做出要求，防止被盗用。

Web 服务器本身会存在一些安全上的漏洞，需要及时进行版本升级更新。尽量使 E-mail、数据库等服务器与 Web 服务器分开，去掉无关的网络服务。在 Web 服务器上去掉一些不用的如 Shell 之类的解释器。定期查看服务器中的日志文件，分析一切可疑事件。设置好 Web 服务器上系统文件的权限和属性，通过限制许可访问用户 IP 或 DNS。从公共网关接口 (CGI, Common Gateway Interface) 编程角度考虑安全，CGI 是外部应用程序 (CGI 程序) 与 Web 服务器之间的接口标准，是在 CGI 程序和 Web 服务器之间传递信息的规程，用来解释处理来自表单的输入信息。采用编译语言比解释语言会更安全，并且 CGI 程序应放在独立于超文本标记语言 (HTML, HyperText Markup Language) 存放目录之外的 CGI-BIN 下。

## 2. SQL 注入攻击的防御

SQL 注入攻击的防御方法有很多种，比较常见的有下列 16 个方面。

(1) 将输入中的单引号变成双引号。这种方法经常用于解决数据库输入问题，同时也是一种对于数据库安全问题的补救措施。不过，有时候，攻击者可以将单引号隐藏掉。比如，用“char(0x27)”表示单引号。所以，该方法并不是解决所有问题的方法。

(2) 用户输入验证。即验证用户输入是否合法，是否会对系统造成攻击行为，包括白名单验证和黑名单验证。白名单是设置能通过的用户；黑名单是设置不能通过的用户。

(3) 认真对表单输入进行校验，从查询变量中滤去尽可能多的可疑字符。可以利用一些手段，测试输入字符串变量的内容，定义一个格式为只接受的格式，只有此种格式下的数据才能被接受，拒绝其他输入的内容，如二进制数据、转义序列和注释字符等。另外，还可以对用户输入的字符串变量进行类型、长度、格式和范围进行验证并过滤，也有助于防治 SQL 注入攻击。通过部署 Web 防火墙、IPS 等设备，监控并过滤恶意的外部访问，并对恶意访问进行统计记录，作为安全工作决策及处置的依据。

(4) 在程序中，组织 SQL 语句时，应该尽量将用户输入的字符串以参数的形式进行包装，而不是直接嵌入 SQL 语言。由于很多 SQL 注入都是把用户输入和原始的 SQL 语言嵌套组成查询语句来完成攻击，而参数不能被嵌套进入 SQL 查询语言，因此，该种措施可以在某种程度上防止 SQL 注入。不过，在不同的语言和产品里面，做法稍有不同。

(5) 摒弃动态 SQL 语句，而改用用户存储过程来访问和操作数据。这需要在建立数据库后，仔细考虑 Web 程序需要对数据库进行的各种操作，并为之建立存储过程，然后让 Web 程序调用存储过程来完成数据库操作。这样，用户提交的数据将不是用来生成动态 SQL 语句，而是确确实实地作为参数传递给存储过程，从而有效阻断了 SQL 注入的途径。

(6) 严格区分数据库访问权限。在权限设计中，对于应用软件的使用者，一定要严格限制权限，没有必要给他们数据库对象的建立、删除等权限。这样，即使在收到 SQL 注入攻击时，有一些对数据库危害较大的工作，如 DROP TABLE 语句，也不会被执行，这将减少注入式攻击对数据库带来的危害。

(7) 多层架构下的防治策略。在多层环境下，用户输入数据的校验与数据库的查询被分离成多个层次。此时，应该采用以下方式进行验证：①用户输入的所有数据，都需要进行验证，通过验证才能进入下一层；此过程与数据库是分离的。②没有通过验证的数据，应该被数据库拒绝，并向上一层报告错误信息。

(8) 对于数据库敏感的、重要的数据，不要以明文显示，要进行加密。

(9) 对数据库查询中的出错信息进行屏蔽，尽量减少攻击者根据数据库的查询出错信息来猜测数据库特征的可能。

(10) 由于 SQL 注入有时伴随着猜测，因此，如果发现一个 IP 不断进行登录或短时间内不断进行查询，可以自动拒绝他的登录；也可以建立攻击者 IP 地址备案机制，对曾经的攻击者 IP 进行备案，发现此 IP，直接拒绝。

(11) 实时监控保护，即时刻对用户访问 Web 网站时发送的请求进行监控，拒绝所有存在隐患或不符合规范的输入，这样可以做到最大限度地阻止用户进行 SQL 注入攻击。

(12) 事件应急响应。提前做好发生概率较大的安全事件的预案及演练工作，力争以最高效、最合理的方式申报并处置安全事件，并整理总结。

(13) Web 应用安全加固。对应用代码及其中间件、数据库、操作系统进行加固，并改善其应用部署的合理性。从补丁、管理接口、账号权限、文件权限、通信加密、日志审核等方面对应用支持环境和应用模块间部署方式划分的安全性进行增强。

(14) 养成查看日志记录。一旦发生 SQL 注入，在日志记录中会记录下攻击的时间和入侵漏洞，可以使管理员及时处理。对数据库重要的信息进行加密，可采用信息摘要算法 5 (MD5, Message Digest Algorithm 5) 函数进行加密。

(15) 可以使用专业的漏洞扫描工具来寻找可能被攻击的漏洞。

(16) 安全知识培训。让开发和运维人员了解并掌握相关知识，在系统的建设阶段和运维阶段同步考虑安全问题，在应用发布前最大限度地减少脆弱点。

### 3. 跨站脚本攻击 (XSS) 的防御

XSS 攻击最主要目标不是 Web 服务器本身，而是登录网站的用户。针对 XSS 攻击，下面主要从普通浏览网页用户及 Web 应用开发者的角度给出防御建议。

#### 1) 普通浏览网页用户

在网站、电子邮件或即时通信软件中点击链接时需要格外小心：留心可疑的过长链接，尤其是它们看上去包含了 HTML 代码。对于 XSS 漏洞，没有哪种 Web 浏览器具有明显的安全优势。防火墙也同样不安全。为了获得更多的安全性，可以安装一些浏览器插件：比如 Firefox 的 NoScript 或 Netcraft 工具条。世界上没有“100%的有效”。尽量避免访问有问题的站点，比如提供 Hack 信息和工具、破解软件、成人照片的网站。这些类型的网站会利用浏览器漏洞并危害操作系统。

#### 2) 从 Web 应用开发者的角度

对于开发者，首先应该把精力放到对所有用户提交内容 (URL、查询关键字、post 数据等) 进行可靠的输入验证上。也就是说，某个数据被接受之前，必须使用一定的验证机制来验证所有输入数据，如长度、格式、类型、语法等；常见的方法，比如黑名单验证，就是将一些常见的字符进行过滤。只接受在所规定长度范围内、采用适当格式的字符，阻止、过滤或忽略其他的任何东西。例如，我们可以限制输入的字符数，来阻止那些较长的 script 的输入。另外，还可以用 Javascript 来对字符进行过滤，将一些如 %、<、>、[、]、{、}、;、&、+、-、"、(、) 的字符过滤掉。

对于任意的输出数据，要进行适当的编码，防止任何已成功注入的脚本在浏览器端运行；数据输出前，确保用户提交的数据已被正确进行编码；可在代码中明确指定输出的编码方式 (如 ISO-8859-1)，而不是让攻击者发送一个由他自己编码的脚本给用户。



保护所有敏感的功能，以防被机器自动执行或被第三方网站所执行。可采用的技术有 session 标记、验证码。

如果你的 Web 应用必须支持用户提交 HTML，那么应用的安全性将受到灾难性的下降。但是还是可以做一些事来保护 Web 站点：确认接收的 HTML 内容被妥善地格式化，仅包含最小化的、安全的 tag（绝对没有 JavaScript），去掉任何对远程内容的引用，尤其是 CSS 样式表和 JavaScript。

总体而言还可以采用下列防范手法：

(1) Cookie（小型文本文件）防盗。首先，避免直接在 Cookie 中泄露用户隐私，如 E-mail、密码等。其次，通过使 Cookie 和系统 IP 绑定来降低 Cookie 泄露后的危险。这样攻击者得到的 Cookie 没有实际价值，不可能拿来重放。

(2) 尽量采用 post（浏览器将提交表单中的字段信息放置在请求体中）而非 get（浏览器将提交表单中的字段信息放置在请求头中）提交表单。Post 操作不可能绕开 JavaScript 的使用，这会给攻击者增加难度，减少可利用的跨站漏洞。

(3) 严格检查 refer。检查 http refer 是否来自预料中的 URL。这可以阻止第 2 类攻击手法发起的 HTTP 请求，也能防止大部分第 1 类攻击手法，除非正好在特权操作的引用页上种了跨站访问代码。

(4) 将单步流程改为多步，在多步流程中引入校验码。多步流程中每一步都产生一个验证码作为 hidden 表元素嵌在中间页面，下一步操作时这个验证码被提交到服务器，服务器检查这个验证码是否匹配。首先，这为第 1 类攻击者大大增加了麻烦。其次，攻击者必须在多步流程中拿到上一步产生的校验码才有可能发起下一步请求，这在第 2 类攻击中是几乎无法做到的。

(5) 引入用户交互，简单的一个看图识数可以堵住几乎所有的非预期特权操作。

(6) 只在允许 anonymous 访问的地方使用动态的 JavaScript。

(7) 对于用户提交信息的中的 img 等 link，检查是否有重定向回本站、不是真的图片等可疑操作。

(8) 内部管理网站的问题。很多时候，内部管理网站往往疏于关注安全问题，只是简单的限制访问来源。这种网站往往对 XSS 攻击毫无抵抗力，需要多加注意。

XSS 攻击相对其他攻击手段更加隐蔽和多变，和业务流程、代码实现都有关系，不存在什么一劳永逸的解决方案。此外，面对 XSS，往往要牺牲产品的便利性才能保证完全的安全，如何在安全和便利之间平衡也是一件需要考虑的事情。

#### 4. 网页挂马的检测与防治

网页挂马常见的检测方法有：①网页挂马可以用专业免费网页安全检测工具横向测评，如 McAfee SiteAdvisor 等；②可以利用百度、Google 等搜索引擎搜索网站，如果网站有木马则搜索引擎会在搜索列表的下方提示有不安全因素，这就说明网站有可能被挂马

了；③也可以利用杀毒软件进行查杀网页源文件，如果发现木马程序，则说明网站源代码中存在网页挂马现象，此时也可以手动清除木马，也可以在站点中发现相同特征木马，将其全部替换成空格即可；④人为判断方式，通过在客户端浏览页面，如果发现大量<js>或<iframe>标签，里面还含有与本站无关的网址，则很有可能网站被挂木马，也可以手动在服务器端清除。

要想使网站安全运营，除了会找出木马并清除之外，还应该养成良好的维护习惯和备份习惯，具体做法下面加以详细介绍。

(1) 更新补丁。大部分网页木马会利用 IE 等浏览器的漏洞来进行进攻，一个比较简单的方式就是及时地更新补丁，以防止黑客利用漏洞对服务器端口探测、SQL 注入、篡改密码、权限提升等操作。

(2) 更改系统的环境变量。在操作系统中有一个环境变量，在这里可以定义常见应用程序的路径。如果我们在这里将一些比较危险的应用程序的路径去掉，那么木马就会因为找不到可以运行的平台而无疾而终。可以在操作系统的环境变量中，找到 PATHEXT 变量名，将这里面的一些经常容易被网页木马利用的变量值删除。如可以将 VBS、JS 等内容删掉。这些变量是木马经常使用的。

(3) 要养成看网页源代码的习惯。无论多高明的网页木马，都会在源代码中看出一点端倪。通过代码，可以了解木马的工作原理、变现形式、欺骗的手段以及未来的发展趋势等。当我们发现可疑网页，可以点击工具栏上的“查看”按钮，然后选择源文件，就可以看到这个网页的源代码。

(4) 禁用危险的端口与服务。在默认情况下，IE 启用的端口数量会比较多，但是也带来了很多的安全隐患。很多木马就喜欢使用这些途径来发起攻击。如 FTP、TFTP (Trivial FTP) 这些服务，对于普通用户来说，基本上用不着。而这些服务以及对应的端口就可能成为木马发动攻击的漏洞。为此在必要的情况下，需要禁用 FTP 等服务的端口，防止网页木马利用这些途径来发起攻击。当用户有需要的时候，管理员可以再替用户打开。

(5) 日常操作中要引起警觉。要注意其网页地址的格式，一旦发现 IE 运行不正常，如速度比较慢或自动关闭等，需要及时的告知安全管理人员，必要时对用户访问的网页进行监控。

(6) 网站后台登录入口可以在首页隐蔽位置做小链接或根本不做链接。记住后台登录地址和路径，可以有效防止黑客嗅探，黑客运用社会工程学猜测账号密码。

(7) 在站点中写入一些有效防止挂马的代码。使得一些挂马代码不被执行和运作。

(8) 经常对网站源代码进行更新和检查。一旦发现异常代码，马上快速仔细地清除之。

(9) 要防止利用 U 盘等移动设备在多网和多台计算机之间进行拷贝。

(10) 最有效的办法就是养成备份的好习惯。就是不定期地对服务器系统、网站数据库、网站主程序、网站中的上传文件夹、图片等做备份，一旦黑客攻击网站或网站

挂马难以清除，可以快速高效地恢复到原始状态，这也是作为一个网络管理人员必备的素养。

### 7.3.6 数据恢复技术手段

#### 1. 定义

数据恢复就是把遭受破坏或由硬件缺陷导致的不可访问、不可获得或由于误操作等各种原因而丢失的数据还原成正常数据，即恢复至本来“面目”。它是指通过技术手段，将保存在台式机硬盘、笔记本硬盘、服务器硬盘、存储磁带库、移动硬盘、U 盘、数码存储卡、MP3 等设备上丢失的电子数据进行抢救和恢复的技术。

数据恢复过程主要是将保存在存储介质上的资料重新拼接整理，即使资料被误删或硬盘驱动器出现故障，只要在存储介质的存储区域没有严重受损的情况下，还是可以通过数据恢复技术将资料完好无损地恢复出来。

数据恢复是出现问题之后的一种补救措施，它既不是预防措施，也不是备份措施。删除、格式化等硬盘操作丢失的数据是可以恢复的，上述简单操作后数据仍然存在于硬盘中，懂得数据恢复原理知识的人只需几下便可将消失的数据找回来。但是，在一些特殊情况下数据将很难被恢复，如数据被覆盖、低级格式化清零、磁盘盘片严重损伤等。

#### 2. 常见种类

##### 1) 软恢复

所谓软恢复是指一切可以通过“软”的方式进行的恢复，如由恶意的程序、恶意的破坏、操作系统或应用软件的错误、病毒感染、误格式化、误分区、误克隆、误操作、误删除、网络破坏、黑客攻击、操作时断电、硬件失效、文件加密后密码遗忘、内存溢出、升级等引起，一般表现为系统不能正常启动、无操作系统、读盘错误、文件找不到或打不开、无法进入系统、磁盘出现坏道、分区表丢失、BOOT（引导）区丢失、主引导记录（MBR，Main Boot Record）区丢失、未格式化、密码丢失、乱码、Office（Word、Excel、Access、PowerPoint）系列文件损坏、数据库损坏、邮件损坏等情况下的数据恢复。

##### 2) 硬恢复

一切涉及硬件修理，由硬件损坏或失效造成的数据恢复均归入硬恢复，如由磁头烧坏、磁头老化、磁头芯片损坏、磁道损坏、磁盘划伤、磁组损坏、电机损坏、磁头偏移、零磁道坏、大量坏扇、盘片划伤、磁组变形、电路板损坏、芯片烧坏、断针断线、固件信息丢失、固件损坏及其他元器件烧坏等引起，一般表现为不认盘、常有一种“咔嚓咔嚓”的磁头撞击声、电机不转、通电后无任何声音、读写数据错误、启动困难、经常死机、格式化

失败等情况下的数据恢复。

两者之间最明显的特征或区别就是：存储介质本身是否需要进行治疗或更换部件才可以进行正常的访问。

### 3. 常用的数据恢复软件

常用的数据恢复软件主要有蓝梦软件（BestRecovery）、效率源（Data Compass）、salvationdata、PC-3000、Final Data、安易数据恢复软件（EasyRecovery）、PTDD、WinHex、R-Studio、DiskGenius、RAID Reconstructor、迅捷数据恢复、易我数据恢复向导等。

EasyRecovery 对于分区破坏和硬盘意外被格式化都可安全地恢复，所要做的就是将数据损坏硬盘挂到另外一台计算机上，尽情恢复就是了，不过 EasyRecovery 对于中文的文件名和目录名效果不是很好。EasyRecovery 支持从各种各样的存储介质恢复删除或丢失的文件，其支持的媒体介质包括硬盘驱动器、光驱、闪存、硬盘、光盘、U 盘/移动硬盘、数码相机、手机和其他多媒体移动设备。其功能包括硬盘数据恢复、Mac 数据恢复、U 盘数据恢复、移动硬盘数据恢复、相机数据恢复、手机数据恢复、MP3/MP4 数据恢复、光盘数据恢复、其他超级光盘（SD，Super Disc）卡数据恢复、电子邮件恢复、独立冗余磁盘阵列（RAID，Redundant Array of Independent Disk）数据恢复，支持所有文件类型的数据恢复，能够识别多达 259 种文件扩展名。

安易数据恢复软件是一款新的数据恢复软件，其功能不亚于一些老牌恢复软件甚至超过其他恢复软件功能。

迅捷数据恢复软件主要功能用于恢复删除文件、恢复被格式化的文件、恢复丢失的分区中的文件，以只读方式从介质底层读取原始数据，不会对介质进行任何写入操作，不产生二次破坏。这种软件完美兼容 Win7/8/XP/Vista/2000 等 Windows 系统；支持 FAT/FAT32/NTFS/exFAT 等文件系统；支持硬盘/U 盘/SD 卡/移动硬盘/手机内存卡等存储介质；支持 Word/Excel/PPT/JPG/MP3/MP4/AVI/RAR/ZIP/EXE/TXT 等 200 多种文件格式。

蓝梦软件（BestRecovery）是蓝梦软件研发中心研发的一系列数据恢复软件。它集合了近十年的数据恢复经验和文件系统及文件类型存储结构算法，完美支持删除、格式化、误 Ghost、重新分区、病毒破坏、文件系统损坏等。

R-Studio 是功能超强的数据恢复、反删除工具，采用全新恢复技术，为使用 FAT12/16/32、新技术文件系统（NTFS，New Technology File System）（Windows NT 家族）、NTFS5（Windows 2000 系统）和 Ext2FS（Linux 系统）分区的磁盘提供完整数据维护解决方案。同时提供对本地和网络磁盘的支持，此外大量参数设置让高级用户获得最佳恢复效果。具体功能有：采用 Windows 资源管理器操作界面；通过网络恢复远程数据；支持 FAT12/16/32、NTFS、NTFS5 和 Ext2FS 文件系统；能够重建损毁的 RAID 阵列；为磁盘、分区、目录生成镜像文件；恢复删除分区上的文件、加密文件（NTFS5）、数据流（NTFS、NTFS5）；恢复 FDISK（DOS 外部命令，给硬盘分区或查询硬盘分区状况）或其他磁盘工具删除过的数据、病毒破坏的数据、MBR 破坏后的数据；识别特定文件名；把数据保存到任何磁盘；浏览、编辑文件或磁盘内容等。

#### 4. 数据恢复的基本操作步骤

##### 1) 询问客户

接到硬盘后，应向客户询问数据丢失的类型，是误删除，误格式化，误分区，意外丢失，还是硬盘突然丢失或无法读写，并且还要询问故障发生后，客户自己还做过哪些操作。把故障类型和原因问清楚了，可能会减少我们在数据恢复过程中一些不必要的麻烦，提高工作效率。

##### 2) 硬盘外观检测

对于硬件问题造成的数据丢失，这时我们应首先检查硬盘的电路板有无明显的烧灼痕迹，避免因该硬盘的电路损坏再次造成计算机主机的损坏。

##### 3) 加电试盘

如硬盘无明显的电路损坏，把硬盘加电试机，在互补金属氧化物半导体（CMOS，Complementary Metal Oxide Semiconductor）中是否能够找到硬盘。

##### 4) 根据故障类型选用合适的的数据恢复工具

如果能够找到硬盘，就按软件方面使用 EasyRecovery 之类的软件进行数据恢复。如果找不到硬盘，就按硬件故障的方法进行处理。

##### 5) 将数据转移安全区域

把找回的数据拷贝到另一块物理硬盘上，一定不能拷贝在同一块硬盘的不同分区。

##### 6) 移交数据

将数据用刻录机刻成光盘，交给用户。



# 第 8 章

## 网络空间进攻源的追踪

为了有效防御网络空间进攻，人们提出了网络攻击追踪溯源技术，用于跟踪信息在网络上流传的轨迹，定位攻击源头，以便追查攻击者，并采取隔离或其他手段阻止或遏制网络攻击，将网络攻击的危害降到最低。这对于防御方能够实施针对性的防护策略，缔造一个安全可信的网络环境，提高网络空间领域犯罪的破案率、威慑力，为进攻行为责任的判定提供法律举证和依据，并将其绳之以法等方面具有非常重要和积极的意义。为此本章重点分析网络空间追踪各层次问题，并就相应技术及追踪过程进行深入讨论，以期对追踪源有一个全面的描述，提高对网络攻击源追踪的认识。

### 8.1 网络空间作战进攻源追踪概述

#### 8.1.1 网络空间进攻源追踪的概念与作用

“追”有赶、紧跟着、回溯过去、补做过去的事、竭力探求和寻求的意思。“踪”是人或动物走过留下的脚印。“追踪”原意是指按踪迹或线索追寻或追随仿效。

“追踪”一词，其英文是 `traceback`。`Traceback` 在国内文献中多翻译为追踪、源路由追踪、反向追踪、溯源、回溯等，虽然名目繁多，但表达的内容却是一致的。本章采用进攻源追踪这种表达方式。

网络空间进攻源追踪是指在网络空间作战过程中，通过一定的技术手段、方法和收集相关信息，将网络空间进攻行为追溯到该行为的发起者；更具体地说就是要找到事件发生的源头、发生的根本原因，识别特定信息的来源，查询网络进攻的元数据和历史状态，推导信息在网络中的遍历路径和过程，确定进攻者的身份、位置和中间介质。身份指进攻者名字、账号或与之有关系的类似信息；位置包括其地理位置或虚拟地址，如 IP 和 MAC 地址、认证的主机名等。

网络空间进攻源追踪技术的研究及应用作用非常显著，具体表现在以下几个方面：

(1) 通过进攻源追踪与定位，能够及时地制定、实施有针对性的防御策略，动态调整网络防护措施，提高网络主动防御的及时性和有效性。

(2) 使得防御方在确定攻击源后可以通过拦截、隔离、关闭等手段将攻击损害降到最低，保证网络健康平稳地运行。

(3) 进攻源定位后，通过多部门配合协调，可将进攻主机进行关闭搜查，从源头保证网络运行安全。

(4) 利用进攻源追踪技术可追踪定位网络内部攻击行为，防御内部攻击。

(5) 利用进攻源追踪技术可对网络攻击过程进行记录，一方面可以为入侵检测系统的事件处理、入侵响应决策、了解和掌握最新攻击方法，以及进一步加强网络安全防范提供有效依据；另一方面在提供法律举证、追究有关责任人、威慑攻击者和打击计算机网络犯罪方面具有非常积极的意义。

(6) 有利于及时了解系统安全状态，有针对性反制或抑制网络攻击。

## 8.1.2 网络空间进攻源追踪的困难与面临的挑战

由于互联网设计之初并没有考虑相应的安全机制，只是为了满足人们的通信交流，其设计是基于可信用户。在真实的网络中直接攻击相对较少，攻击者通常会采取一些用于隐藏自身真实地址或意图的方法后再发动攻击。因此，要在网络中获取真实信息，实现网络源追踪面临非常巨大的困难和挑战。

### 1. 互联网设计之初未考虑追踪用户行为的功能

电话网具备有效的追踪和计费功能，这是由其收费模式决定的，电信公司依据用户每次通话的时长、地点、号码等信息给出账单。但是互联网却没有这样的基础追踪定位联网用户。早期的互联网根本没有考虑对每次主机到主机的连接收费或对每封电子邮件的收发计费，该时期的网络由政府资助，科研人员等用户免费使用网络。现在的网络收费也仅限



于按时段、带宽、存储容量等收费，ISP 不会因为计费而像电话网那样详细记录用户的操作行为。此外，计算机网络设计初衷是开发尽可能多的、有利于研究合作的网络应用，从来没有考虑配置追踪网络行为的功能设施。互联网是无连接的分组数据网，没有电气连接，其设计是基于可信用户群，重点在于防范外部攻击，因此没有考虑记录用户活动、防范不可信用户、抵御内部攻击等方面。

## 2. 数据包源地址的不可信

由于当前的 TCP/IP 协议对 IP 包的源地址没有验证机制，以及互联网基础设施的无状态性，使得想要追踪数据包的真实起点很不容易，而要查找那些通过多个跳板或反射器等实施攻击的真实源地址就更加困难。具体体现在以下 7 个方面。

(1) 当前主要的网络通信协议 (TCP/IP) 中没有对传输信息进行加密认证的措施，况且 IP 地址是一个虚拟地址而不是一个物理地址，攻击者能够对数据源 IP 地址字段直接进行修改，或者假冒，以隐藏其自身信息。对于单向通信而言，攻击者可以直接篡改其地址，填入虚假地址信息；对于双向通信而言，伪造源地址相对更复杂，但相关技术也已被攻击者所掌握，并广泛传播。IP 地址这种伪造欺骗技术，使得以 IP 地址为基础去发现攻击者变得更加困难。

(2) 一种伪造源 IP 地址的攻击方法是在攻击实施前渗透控制数台计算机以作为中间机或跳板，再通过这些受控制的中间机或跳板攻击最终的目标系统，以达到隐藏自身的目的。从被攻击端来看，其看到的数据源是来自不同网域、地址的计算机，而真正攻击者却隐藏在这些计算机后。基于这种方式，还能有不少改进的攻击方式，以最大化地实现攻击者的隐藏，扰乱安全监测，逃避追踪。比如延迟攻击，攻击者在控制了中间机或跳板后，通过在系统内设置特有的定时器等，实现攻击行为的延迟，使攻击追踪更加困难。

(3) 国际互联网已从原来单纯的专业用户网络变为各行各业都可以使用的大众化网络，其结构更为复杂，使攻击者能够利用网络的复杂性逃避追踪。

(4) 各种网络基础和应用软件缺乏足够的安全考虑，攻击者通过俘获大量主机资源，发起间接攻击并隐藏自己。

(5) 一些新技术在为用户带来好处的同时，也给追踪溯源带来了更大的障碍。VPN 采用的 IP 隧道技术，使得无法获取数据报文的信息；网络服务供应商采用的地址池和 NAT 技术，使得网络 IP 地址不再固定对应特定的用户；移动通信网络技术的出现更是给追踪溯源提出了实时性要求，这些新技术的应用都使得网络追踪变得更加困难。

(6) 目前追踪溯源技术的实施还得不到法律保障，如追踪技术中，提取 IP 报文信息牵扯到个人隐私。这些问题不是单靠技术手段所能解决的。

(7) 早期网络规模较小时，每台计算机都分配了静态 IP 地址，但是随着主机数量的增多，IPv4 的 32 位地址只能依靠诸如动态主机配置协议 (DHCP, Dynamic Host Configuration Protocol) 的方式实现地址分配，这帮助计算机攻击者每次联网都能获得不同的 IP 地址。另外，攻击者可以购买无须实名的预存话费手机卡，通过智能手机上网实施攻击，这种情况下即使追踪到手机 IP 仍很难找到攻击者所在地址。

### 3. 网络空间计算机攻击的跨越性

过去的计算机系统和早期的网络都受到集中管控，系统管理员完全控制着自己管理域内所有的系统和网络的软硬件。此外，当时计算机系统的使用者都是可信的雇员，能严格遵守安全规定，因为一旦违规将面临一定惩罚或解雇。现在的互联网连通了数不尽的各种部门机构管理着的域内的计算机，每个管理域由一个机构或个人管理，但是没有一个中心管理机构或实体能够承担监管整个互联网的重任，也没有一个单独的机构或实体能够监视整个互联网上的一举一动，各机构只能通过合作实现对其管理域之外数据包的监控和追踪。网络空间在跨越各种传统边界（行政管理、法律、国家）的同时，对追踪和制裁攻击者造成了极大不便。

### 4. 网络传输的高带宽

从用户角度看，使用的网络带宽越高越好，高带宽意味着路由器必须尽可能快地传输大量数据包，而通过路由器对大量数据包进行分析和标记，以便追踪攻击源的做法只能使路由器的吞吐能力极度下降。另外，高带宽大大缩短了追踪所需的数据包信息的有效存储时间，因为路由器单位时间内传输的大量数据包很快就能写满存储设备，如果对攻击行为追踪的速度不够迅速，相关信息很快就会消失。

### 5. 网络攻击复杂化、工具化增加了追踪难度

在巨大利益的驱使下，网络攻击威胁日益增大，攻击的复杂度不断提升。一些攻击者控制数以万计的僵尸机，在更广泛的网络空域发动攻击，其组织结构复杂，追踪难度巨大；一些攻击者悄悄潜入系统，完成其既定行动后，悄悄地离开，看不到任何痕迹，追踪无从查起；还有一些攻击者，采取更为巧妙的技术，在一个相当长的周期内实施攻击，由于时间上跨度大，相关数据流关联性差等特点，很难对其进行追踪定位。同时，计算机技术的普及，一些网络扫描、漏洞利用等网络攻击软件工具化趋势明显，使网络攻击门槛降低，网络攻击自动化、傻瓜化，网络威胁事件急剧增加，增加了网络攻击追踪的难度和复杂度。

### 6. 政治和经济利益阻碍网络协同，阻碍攻击追踪

目前，发起的网络攻击总是跨越多个网域甚至国家。追踪如此大范围的攻击行为，确定真正攻击者，需要各网域的网络管理机构进行协同，需要各国配合，才能实现，以至将犯罪分子绳之以法。然而，由于世界各个政治、经济、文化的差异以及利益的不同，国家间的配合难以有效应对网络攻击事件；各网络供应商更是为了保护技术、经济上的利益鲜有协作，这些都直接阻碍了网络攻击追踪的实施，无法进一步追踪定位攻击源。

### 7. 个人隐私保护和法律法规不健全阻碍攻击追踪应用

通过网络人们可以办理政务、金融和购物等多种事务，而这其中涉及不少个人隐私。随着个人信息保护意识的增强，人们对个人隐私的保护越来越重视，不少网络攻击的目标

就是个人隐私信息，并将其出售而获取利益。人们一方面越来越依赖于网络社会，另一方面面对网络攻击追踪技术的应用心存疑虑，担心个人的隐私信息被追踪而暴露。这使得这些人更容易受到网络攻击，并增强攻击所造成的破坏性影响，这也反映了网络攻击追踪技术应用的困境。

8.1.3 网络空间进攻源追踪的分类

网络空间进攻源追踪内涵丰富、应用广泛，其研究涉及许多方面，因此，根据不同的内容可以进行不同的分类。

1. 按照追踪的深度和精准度分类

网络空间进攻源追踪按照追踪的深度和精准度可以分为四个层次：

- 第一层：追踪攻击主机；
- 第二层：追踪攻击控制主机；
- 第三层：追踪攻击者；
- 第四层：追踪攻击组织机构。

1) 第一层（追踪攻击主机）

第一层追踪攻击主机的目的是定位攻击主机，即直接实施网络攻击的主机。其追踪问题可用图 8-1 来描述。

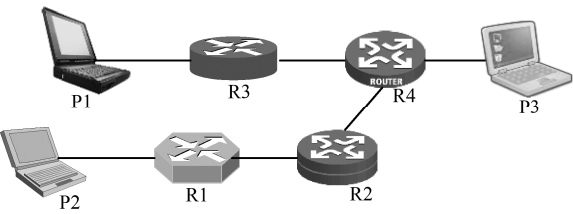


图 8-1 第一层追踪问题描述

网络数据 S 由 P1 产生，通过 R3→R4 传输到接收端 P3，第一层追踪问题可描述为，给定数据 S，如何确定 P1 的问题。

2) 第二层（追踪攻击控制主机）

第二层追踪的目标是确定攻击控制主机。网络攻击者为掩盖身份信息往往利用僵尸网络、匿名通信系统或跳板链进行隐蔽攻击活动，使得攻击源追溯变得异常困难。第二层追踪问题抽象示意图如图 8-2 所示。比如说，给定某一计算机上的事件 1，第二层追踪的目标就是寻找某个“因果关系”的事件，其导致了该计算机上事件 1 的发生。一般来说，这

种“因果关系”是由按某种顺序组合的一系列计算机链路。实际上，这种因果关系就是一种控制关系，这种控制关系可以是多对多，也可能是一对多，甚至是多对一的控制关系。

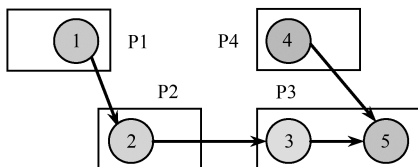


图 8-2 第二层追踪问题抽象示意图

图 8-2 中，将计算机抽象成矩形方框，事件用圆圈表示，事件的因果关系使用带箭头的线段表示。图中，攻击者在计算机 P1 处触发事件 1 入侵计算机 P2，并利用 P2 的事件 2 入侵 P3，在 P3 中触发事件 3。而攻击者可以通过计算机 P4 的事件 4 向 P3 发起一个激励或命令，联合或直接启动事件 3 导致事件 5 的发生。需要说明的是，这些事件不需要同时发生。在事件 5 发生时，或许事件 1、2、3、4 已经完成并停止活动。追踪者最初只看到事件 5 的发生和其导致的结果。第二层追踪溯源的目标正是如何通过事件 5 的发生找到其最初的诱因，即事件 1。

第二层追踪采用的技术主要有内部监测、日志分析、快照、数据流分析、数据流水印、事件响应分析等技术。

### 3) 第三层（追踪攻击者）

第三层追踪的目标是追踪定位网络攻击者，这就要求追踪者必须找到网络主机行为与攻击者（人）之间的因果关系。第三层追踪就是通过对网络空间和物理世界的信息数据分析，将网络空间中的事件与物理世界中的事件相关联，并以此确定物理世界中对事件负责的自然人过程。第三层追踪溯源问题描述示意图如图 8-3 所示。

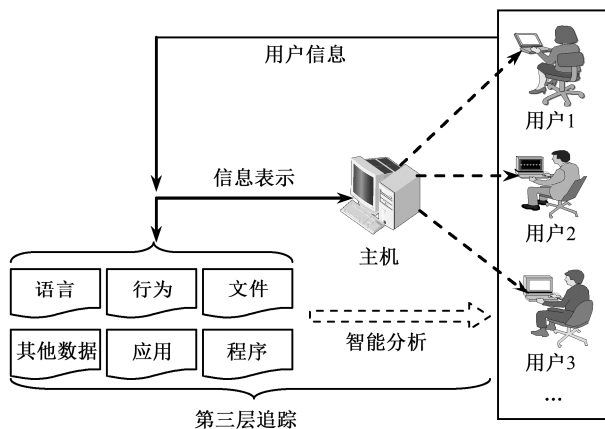


图 8-3 第三层追踪溯源问题描述示意图

第三层追踪包含四个环节：（1）网络空间的事件信息确认；（2）物理世界的事件信息

确认；(3) 网络事件与物理事件间的关联分析；(4) 物理事件与自然人间的因果确认。第一个环节，前两个层次的追踪技术能较好解决。第二个环节需要物理世界中的情报、侦察取证等手段确定。第三个环节是通过网络世界中的信息（主机位置、攻击模式、攻击行为、时间、习惯、文件、语言、键盘使用方式等）与物理世界中取证的各种信息情报进行综合分析，确认网络事件与物理事件的因果关联。在第一层追踪定位攻击源主机基础上，通过获取该主机攻击行为、攻击模式、语言、文件等信息，支持物理世界中的事件确认。第四个环节是采取司法取证等手段，对物理事件中的可疑人员进行调查分析，最终确定事件责任人，即真正的攻击者。

#### 4) 第四层（追踪攻击组织机构）

第四层追踪溯源的目的是确定攻击的组织机构，即实施网络攻击的幕后组织或机构。该层次的追踪问题就是在确定攻击者的基础上，依据潜在机构信息、外交形势、政策战略以及攻击者身份信息、工作单位、社会地位等多种情报信息，分析评估确认人与特定组织机构的关系。第四层追踪溯源问题描述示意图如图 8-4 所示。

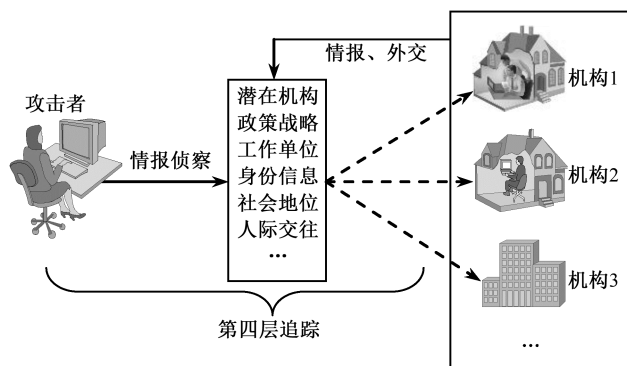


图 8-4 第四层追踪溯源问题描述示意图

第四层的追踪溯源更多的是国家与国家、机构与机构之间的对抗，是网络攻防的一种高级形式。第四层追踪是一个更加复杂的系统工程，但仍以第一层、第二层和第三层追踪为基础。在前三个层次的追踪基础上，结合谍报、外交、第三方情报等所有信息，综合分析评估并确定网络攻击事件的幕后组织机构。

## 2. 从追踪的标志来分类

从追踪的标志来考察，网络空间追踪可以划分为两大类型，即 IP 追踪和 ID 追踪。所谓 IP，指的是联网终端主机的 IP 地址，由于互联网体系架构的开放性，任何一台终端只需配置全球唯一的 IP 即可连入互联网。这也使得 IP 地址成为联网终端的唯一标志，而 IP 追踪的目的亦即找出目标终端的真实 IP 地址并以此为据来追溯网络行为的实际发起者。与 IP 追踪相区别的是 ID 追踪。所谓 ID，是一个笼统的说法，指的是联网用户的一种网络身份标志，比如 E-mail 地址、QQ 号码、论坛注册用户名等。在许多情况下，通过 ID 进

行追踪是一种更有效的方式，因为它更多地利用了社会工程学原理，可以借鉴社会工程学领域已有的追踪经验。在理论研究的范畴里，网络追踪更多的是指 IP 追踪。

### 3. 从追踪的技术来分类

到目前为止，已有的追踪溯源技术大致可分为三大类：主动询问、数据监测和路径重构。

#### 1) 主动询问类

此类方法通过主动询问数据流可能经过的所有路由器，确认其流向路径的机制（Input Debugging）。主动询问是一种比较粗的方法，通过带有 Input Debugging 功能的路由器进行一级一级（Hop-by-hop）的沿攻击数据流路径查询追踪，其原理示意图如图 8-5 所示。有不少的 ISP 通过设备升级改造，安装更加智能的路由器系统提高追踪效率及能力。但是此方法无法满足事后追踪要求，且需要大量的人力及各个 ISP 之间的协作。

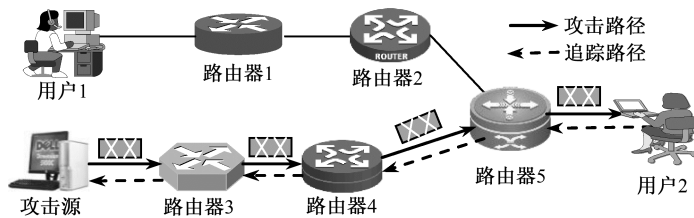


图 8-5 带有 Input Debugging 功能路由器的追踪原理示意图

#### 2) 数据监测类

此类方法通过构建覆盖全网络的监测点对网络中数据流进行监测，如各种日志记录技术，其原理示意图如图 8-6 所示；通过对流经路由器的所有数据包（包括攻击数据包）进行信息存储，一旦发生攻击，由被攻击端发起查询信息，以此确定攻击路径。此方法需要大量的存储计算资源且需要数据库技术支持，但基于 Hash（哈希）算法的日志类方法则可大大减少存储资源的需求。

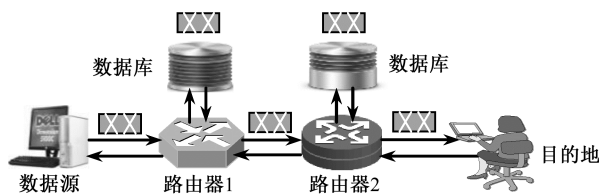


图 8-6 数据监测类追踪原理示意图

#### 3) 路径重构类

路径重构类是目前研究得比较热的一类方法，是追踪技术发展的方向之一，研究产生了大量技术方法及重构算法，其相关理论也较成熟。其核心思想是通过在网络中传输的数

数据包中编入路径信息或单独发送含有路径信息的数据包，接收端通过收集这些包含路径信息的数据包，并根据一定的路径重构算法实现重构攻击数据包路径的目的。较为著名的有概率性包标记（PPM，Probabilistic Packet Marking）、iTrace、确定性包标记（DPM，Deterministic Packet Marking）等，图 8-7 为 PPM 路径重构类追踪的原理示意图。

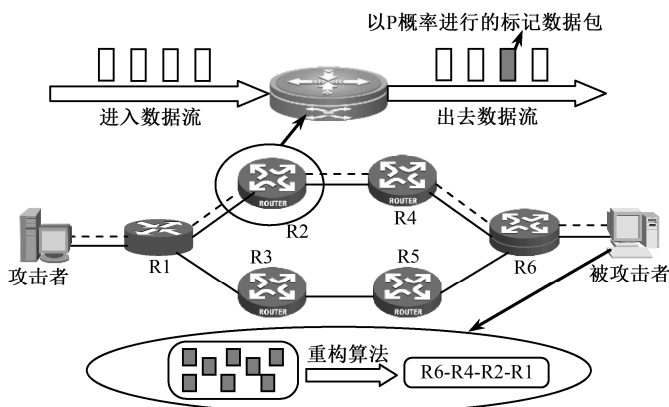


图 8-7 PPM 路径重构类追踪原理示意图

#### 4. 从攻击源隐藏真实地址来分类

目前，针对攻击者所采用的两种隐藏真实地址的方法，网络攻击源追踪问题也相应地分成两大类：一类是 IP 追踪技术，目的是识别发送数据包的真实 IP 地址，该类技术主要是在一系列路由和网关的帮助下在网络层执行。IP 追踪技术的主要方法有连接测试、日志记录、ICMP 追踪、报文标记法等。另一类是面向连接链追踪，目的是识别通过“跳板”隐藏身份的真正攻击源。面向连接链追踪又可以分为三类：基于网络的连接链追踪、基于主机的连接链追踪和基于主动网络的连接链追踪。

### 8.1.4 网络进攻源追踪的信息及其获取

#### 1. 网络入侵的痕迹

网络攻击者在实施攻击之时或之后，必然会留下一些蛛丝马迹和虚拟证据，如何正确处理这些问题是追踪网络攻击的最大挑战。

- (1) 系统日志——缓冲溢出等攻击可在此留下痕迹。
- (2) 服务日志——对服务的攻击会在日志中留下痕迹。
- (3) 电子邮件——有的入侵是通过邮件载入木马的。
- (4) Cookies——可从 Cookie 和历史文件中找出网页类攻击的痕迹。
- (5) 系统进程——木马程序会在进程、端口及其库文件中留下痕迹。

- (6) 网络连接——在网络连接中可能找到黑客入侵痕迹。
- (7) 注册表——从中可以找到木马程序的痕迹。
- (8) 命名管道——可能找到黑客使用的可疑管道。
- (9) 内核——可能存在被入侵者改变的内核配置信息。
- (10) 用户信息——入侵者建立用户账号时留下的痕迹。
- (11) 共享资源——入侵者建立共享链接时留下的痕迹。
- (12) 其他信息——在垃圾箱、程序组、注册服务等中留下的入侵痕迹。

## 2. 进攻源追踪的信息

### 1) 网络数据流

数据流是网络中按照规定的格式组织起来的一串数字编码，用于在网络中通信实体间的信息交互。规定的格式也就是所指的网络通信协议，比如 TCP/IP 协议。有时候人们也把它叫作网络数据流。

网络追踪的数据流主要有：①上网时间，即开始时间和结束时间；②上网地点，即信息点编号或上网电话号码；③上网主机，即 IP 地址和 MAC 地址；④用户，即用户账号。其中 IP 地址是核心数据。追踪者可以采取一定的技术手段获取数据流，进行正确分析数据流，从中能够获知数据来自哪里，数据属于恶意行为还是正常通信等。

获取数据流的手段也叫网络抓包，目前市面上有许多抓包工具，比如 sniffer、wireshark、TcpDump 等。追踪者使用这些抓包工具，将网络接口设置在监听模式，便可以将网上传输的数据信息截获。网络抓包技术广泛地应用于网络故障诊断、协议分析、应用性能分析和网络安全保障等各个领域。

### 2) 日志信息

为了维护自身系统资源的运行状况，网络系统中的信息设备（包括计算机、路由器、入侵检测设备等）一般都会有相应的日志信息，这些信息会记录系统有关日常事件或误操作警报的日期及时间戳等情况。

所谓日志（Log）是指系统所指定对象的某些操作和其操作结果按时间有序的集合。每个日志文件由日志记录组成，每条日志记录描述了一次单独的系统事件。通常情况下，系统日志是用户可以直接阅读的文本文件，其中包含了一个时间戳和一个信息或子系统所特有的其他信息。日志文件为服务器、工作站、防火墙和应用软件等 IT 资源相关活动记录必要的、有价值的信息，这对系统监控、查询、报表和安全审计是十分重要的。日志文件包括系统登录、应用登录、验证、授权和账户（AAA，Authentication, Authorization and Accounting）登录[比如远程用户服务拨号认证(RADIUS, Remote Authentication Dial In User Service) 登录]、网络单元登录、防火墙登录、主机 IDS（HIDS, Host IDS）事件、网络 IDS（NIDS, Network IDS）事件、磁盘驱动器、备份文件、电话记录等。日志文件中的



记录可提供以下用途：监控系统资源，审计用户行为，对可疑行为进行告警，确定入侵行为的范围，为恢复系统提供帮助，生成调查报告，为打击计算机犯罪提供证据来源。

### 3) 恶意代码

恶意代码是指故意编制或设置的、对网络或系统会产生威胁或潜在威胁的计算机代码，能使计算机按照攻击者的意图运行以达到恶意目的的指令集合。这些指令集合包括二进制执行文件、脚本语言代码、宏代码、寄生在文件或启动扇区的指令流。具体表现形式有计算机病毒、蠕虫、恶意移动代码、后门、逻辑炸弹、特洛伊木马、僵尸程序、内核套件（Rootkit）等。

恶意代码具有以下共同特征：①恶意的目的；②本身是计算机程序；③通过执行产生破坏等危害效果。

在网络攻击追踪过程中，追踪者可以对恶意代码进行逆向分析，从中确定攻击目的、攻击时序以及攻击命令控制机制等。这些信息对确定攻击来源以及攻击者身份非常关键。逆向分析也叫逆向工程，大意是根据已有的东西和结果，通过分析来推导出具体的实现方法。比如你看到恶意程序或网络攻击达到的效果，通过反汇编、反编译和动态跟踪等方法，分析出其具体的实现过程，这种行为就是逆向分析。恶意程序逆向分析有多种方法，主要有以下两个方面。①分析网络信息交换监测；②反汇编、编译和调试。

### 4) 主动生成的追踪信息

追踪者根据具体的追踪场景或技术手段还能够主动标记或发送带有追踪信息（包含路径信息）的数据包用于追踪。比如 iTrace 追踪技术就是在网络路由节点处，将路由节点信息及传输数据的摘要以 ICMP 数据包的形式发送到接收端。追踪者需要对这些带有路径信息的 ICMP 数据包进行分析，重构数据传输的路径。在包标记追踪算法中，通过改造路由器的处理过程，将路由节点信息标记在传输的数据流中，追踪者在实施追踪时，读取这些路径信息，进行合理运算，重构数据传输路径。不管是 ICMP 还是包标记中的追踪信息，都是根据具体的网络追踪应用，进行合理设计，主动生成追踪信息数据，用于追踪过程。

另外一类主动生成追踪信息的追踪技术是包标记。该类技术在网络路由节点部署的特定功能的设备或软件，对通过路由节点的数据包标记（比如概率包标记，以概率为 1/20 000），利用 IP 数据包中预留的字段，将数据的网络传输路径信息进行标志记录处理，使得数据中包含路径信息，在被攻击者端接收标记处理的数据包，通过重构路径算法，重构数据网络传输路径。

## 3. 追踪信息的获取

（1）局域网中的数据获取方式主要有：①利用用户上网认证系统，可获得用户账号、上网时间及使用 IP 地址的记录；②利用 DHCP 服务器日志，可获得当前 IP 地址与使用它

的计算机之间的对应表；③利用交换机及路由器，可获得 MAC 地址和 IP 地址；④利用网络布线文档，可获得用户所在的具体上网地点。

(2) 利用 RADIUS 服务器获取信息。RADIUS 是一种用于在需要认证其链接的网络访问服务器 (NAS, Network Access Server) 和共享认证服务器之间进行认证、授权和记账信息的文档协议。RADIUS 服务器通常是 ISP 可以为网络追踪提供记录的唯一设备，它可以确定在某个特定时间，是哪个登录用户名在使用哪个 IP 地址。ISP 一般会将 RADIUS 记录信息保留至少一年。拨号上网是一种互联网访问手段，ISP 一般通过 RADIUS 协议支持拨号路由器和被称为 RADIUS 服务器的中央用户目录之间的验证请求。拨号时，首先是用户端的 Modem 与 ISP 入网点 (POP, Point Of Presence) 中的一个 Modem 建立连接，接着后者直接连接到一个拨号路由器。拨号路由器提示用户输入登录名及口令，确认正确后，由这个路由器分配一个 PPP 连接及一个 IP 地址。RADIUS 服务器有一个集中的目录包含所有用户及其加密口令的列表，记录的内容包括：每次的登录尝试，无论是成功的登录还是失败的登录；每次 logoff 或会话结束的相关信息，这些信息有助于 ISP 跟踪用户的连接时间；每次会话中分配的 IP 地址以及登录者的 ID 名、电话号码。

(3) 利用电子邮件的信息头获取信息。电子邮件的特征是用简单的应用协议和文本存储转发。E-mail 的信息头可读，头信息中包含了从发送者到接收者之间的路径，信息主体完全由可打印字符组成。POP3 协议的邮件仅存储在收信主机上。基于网页进行发送和接收的 HTTP 协议将发送和接收到的邮件存储到服务器上。

从 E-mail 信息头中信息发送路径上的痕迹进行分析可以获取发送者、接收者、发送时间、接收时间、发送地点、接收地点，以及经由的服务器地址等信息。文件头中最重要的线索位于开始位置的一行，它表明该邮件最初源自哪个计算机。另外的信息行表明了此邮件经过了多少个中继服务器，因为每次 SMTP 服务器接收到一个邮件，都会在信息头部添加自己的接收信息域再转发邮件到下一个地址。

通过 Telnet 到 SMTP 服务器的 25 端口手工发送邮件信息，可以插入任何信息到要发送的邮件的信息头中——包括伪造的源地址和目标地址，也可在配置邮箱时选择手工输入发信人地址。由于 SMTP 没有强壮的认证机制，邮件信息的可信度不高。这时候，可以对每个域都执行一个 Nslookup 操作，尤其是名义上的初始域，也就是最后一个接收域，目的是看看它们是否真正存在。然后再对这些域执行 Whois 工作，看看它的管理员是谁，并进一步与之联系。

侦破有关 E-mail 的犯罪案件，ISP 的帮助是必需的：ISP 的电子邮件服务器都具有日志功能，这些日志要比从客户端邮件程序看到的邮件信息头内容更可靠，再加上 RADIUS 日志和电话记录。

(4) 从日志数据中获取信息。系统的日志数据提供了详细的用户登录信息。在追踪网络攻击时，这些数据是最直接、有效的证据。但是，有些系统的日志数据不完善，网络攻

击者也常会把自己的活动从系统日志中删除。因此，需要采取补救措施，以保证日志数据的完整性。防火墙和 IDS 日志可查找一个用户从登录到退出的全部行为。

### 8.1.5 进攻源追踪机制的性能评价指标

现有的一些进攻源追踪定性评价指标包括以下 10 个方面。

(1) 追踪性能。它包括对于不同进攻类型的误报（即将实际没有参加进攻的链路包含在重构的进攻路径中）和漏报（即未将实际参加进攻的链路包含到重构的进攻路径中）。这个性能和进攻的发现能力、对进攻事件的综合分析能力、参与追踪的主体之间的协调能力有密切的关系。

(2) 最小数据量。最小数据量是指能完成网络攻击追踪或攻击路径重构所需的最低数据量。此数据量与所采用的追踪方法、网络结构、攻击模式等有关。在理论上，最小数据量越小越好，它表明追踪者可以根据较少的数据就能够分析出攻击源头的的能力。

(3) 计算复杂度。计算复杂度是指完成网络攻击追踪或攻击路径重构所需要的计算量。对特定的追踪技术来说，其计算复杂度越小越好；但是计算复杂度与重构算法设计、网络资源等多个方面有关。在设计实现时，需要在网络资源（路由器等）、计算资源等多个方面进行折中考虑。

(4) 适应性。适应性是指网络攻击追踪技术的网络适应性、可部署性和可扩展性能力。网络适应性也可以说成兼容性，是否与现有网络协议和架构兼容，是否能够直接应用在前面的网络中。可部署性，讲的是技术是否能够在目前的网络系统中部署应用。可扩展性是追踪技术是否能够方便支持各种新的通信协议及网络技术，是否具有线性扩展性、可升级性、在不断扩大规模的网络中能否很好适用。

(5) 时效性。它包括发现进攻到追踪到进攻源的时延，发现进攻后可以追查进攻源的时限（也就是追踪过程必须在进攻结束之前完成，还可以进行事后分析和追踪）等。越短的追踪时间能够更快地确定攻击源头，从而能够为安全系统应急响应提供更多的防护准备时间，更能有效遏制攻击的进一步扩散，减少攻击所带来的损害。学术界，更多的说法是追踪收敛时间。

(6) 网络资源消耗。网络资源消耗是指网络攻击追踪技术对网络资源的消耗，这里的网络资源主要是指网络带宽，路由开销。比如基于 ICMP 的 iTrace 追踪技术，由于会额外产生用于追踪溯源的 ICMP 数据包，增大了网络流量，占据了额外的网络带宽；再比如基于包标记的追踪技术，在路由节点处，对通过的数据包进行标记处理，将路由节点信息或路径信息标记在网络数据包中以便于后续重构其传输路径。由于在路由器上需要进行额外的信息处理，增加了路由时间，消耗了路由器计算资源，在一定程度上降低了路由器的性能。

(7) 事后追踪。事后追踪是指网络攻击发生结束后，实施的追踪能力。显然，具备事后追踪能力的追踪技术或系统需要首先解决网络数据存储问题，只有将网络攻击实施阶段

的数据存储起来，才能在其结束后进行分析，用于追踪。

(8) 健壮性。健壮性是指少量追踪设备失效对进攻路径重构的影响。如果参与追踪的设备是原来网络本身传输节点，这个性能与原来网络本身的健壮性有很大关系；如果参与追踪的是辅助网络设备，这个有辅助网络设备参加的追踪机制对健壮性有直接的影响。

(9) 自身安全。自身安全指追踪技术自身抗攻击的能力。网络攻击追踪最好对攻击者是透明的，攻击者无从知晓自己是否被追踪，而同时攻击者也不能直接对追踪进行攻击破坏。另外，追踪技术应该考虑对所收集数据进行必要的认证，确保用于追踪的信息数据真实有效，防止追踪数据被伪造、篡改等攻击行为。

(10) 运行性能。进攻源追踪在具体实施过程中的性能，包括对设备更新要求、网络流量负担、参与追踪设备的负载、处理器、内存等占用情况，需要 ISP 的合作、协调管理负担等。

## 8.2 网络空间进攻源追踪的运行机制

### 8.2.1 网络空间进攻源追踪的一般过程

#### 1. 网络追踪的准备阶段

有经验的网络攻击者，在进行网络追踪时一般采取两步走的策略，第一步进行准备工作，第二步才采取具体的追踪行动。

网络攻击者进行网络追踪并不是漫无目的的，而是根据自己的意图，首先确定自己的追踪目标，然后再采取一定的追踪手段进行追踪。在准备阶段，一般分为窃听网络信息、确定可疑对象和收集网络信息三个步骤。可疑的对象不仅指网络中的主机等通信实体，也包括网络流量等信息。网络追踪的准备阶段如图 8-8 所示。

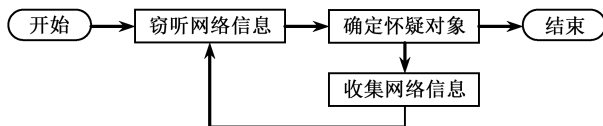


图 8-8 网络追踪的准备阶段

窃听网络信息是一个盲目的过程，在窃听的过程中收集的信息较为杂乱，不能作为追踪的依据。这个阶段主要是为了发现可疑的网络信息，从而初步确定可疑的网络通信实体。这个实体有可能是要识别的通信实体的一方，也有可能是重路由路径中的一跳路由，也有可能是个“无辜者”。追踪者针对这个可疑实体的通信信息进行大量的收集工作，若收集

的信息显示该实体“无辜”，那么追踪者就会放弃该实体的信息收集，重新窃听这个网络信息。如此循环，直到可疑的实体被确定，准备阶段才结束。

## 2. 网络追踪阶段

经过准备阶段后，就要展开网络追踪行动了。网络追踪的过程描述即追踪四层次流程示意图如图 8-9 所示。网络预警系统发现攻击行为请求追踪，对攻击数据流进行追踪定位，分析确定发送攻击数据的网络设备或主机。确定攻击主机后，通过分析该主机输入、输出信息，或其系统日志等信息，判定该设备是否被第三方控制，从而导致攻击数据的产生，据此确定攻击控制链路中的上一级控制节点，如此循环逐级追踪，完成第二层追踪。在第二层追踪的基础上，结合语言、文字、行为等识别分析，可以对追踪者进行分析确定，完成第三层次的追踪溯源。在第三层追踪溯源基础上，结合网络空间之外的侦查及情报等信息，判定攻击者的目的、幕后组织机构等信息，实现第四层追踪溯源。

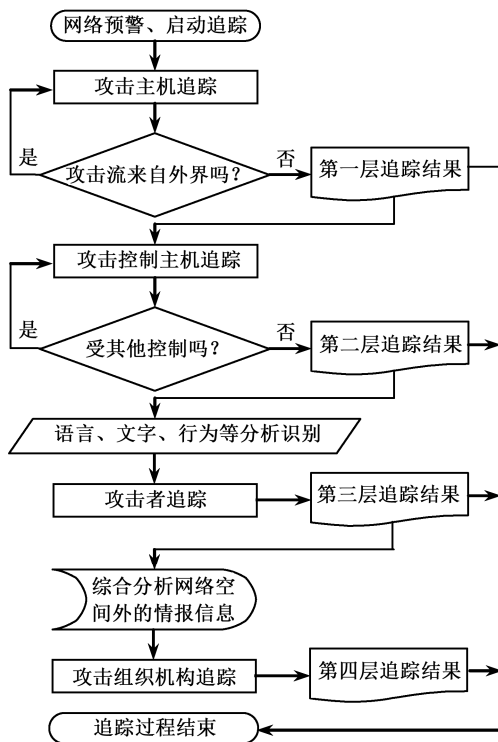


图 8-9 追踪四层次流程示意图

目前，网络追踪第一、二、三层追踪是可以使用相关技术进行信息数据分析，辅助追踪者实现追踪定位。在这三个层次中存在大量亟待突破的技术点和难点，而第四层追踪更多依赖于物理自然世界的综合情报进行推理验证，比如组织机构间的体制、政策、外交、历史等综合信息。特别强调的是，第三层追踪是从网络设备到人的跨越，将设备的控制行为与具体的自然人相关联在技术上具有极大的挑战。

## 8.2.2 系统组件及其功能

### 1. 系统模块及其关系

网络攻击源追踪系统可以分为三个部分，分别是追踪控制模块、报文记录模块和追踪执行模块，追踪系统整体框架及其关系可用图 8-10 来表示。

追踪控制模块是整个系统的中心，负责配置、指挥报文记录部分和追踪执行部分。报文记录模块和追踪执行模块分别完成对数据报文的记录和追踪功能。三个部分协调工作才能完成网络攻击源的追踪工作。

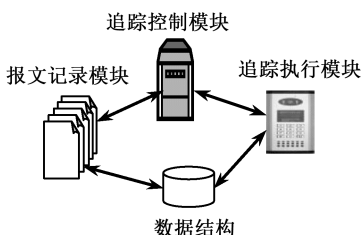


图 8-10 追踪系统整体框架

### 2. 系统节点及其说明

系统节点并不是需要实现的功能模块，这些系统节点都是网络上已经存在的模块与主机，追踪系统及其节点的关系如图 8-11 所示。下面对系统的各类节点做一个说明，方便大家理解。

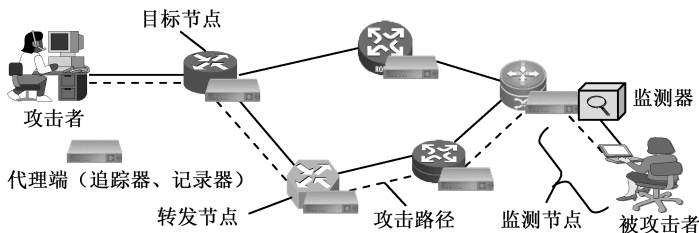


图 8-11 追踪系统及其节点的关系

(1) 目标节点，是指与攻击主机直接相邻的节点（可以是路由器、防火墙或 NAT 设备）。在追踪系统中，一般追踪的最后结果不会是最终的攻击主机，而是攻击主机前面的路由器等设备，只要追踪到这一步，便可以认定已经追踪到攻击源。通常目标节点不止一个。

(2) 监测节点，是监测器所在的网络节点，可以是入侵检测系统或其他类型的主机。根据情况的不同，监测节点有可能就是被攻击主机，也有可能是被攻击主机前面的入侵检测设备、防火墙等。监测节点是攻击源追踪的起点，也是追踪系统最后形成的攻击路径的起点。

(3) 转发节点，是指不与攻击主机和被攻击主机直接相邻的具有报文转发功能的设备，一般情况下是路由器或交换机等设备。

### 3. 系统功能部件及其说明

追踪系统及其功能部件如图 8-12 所示。

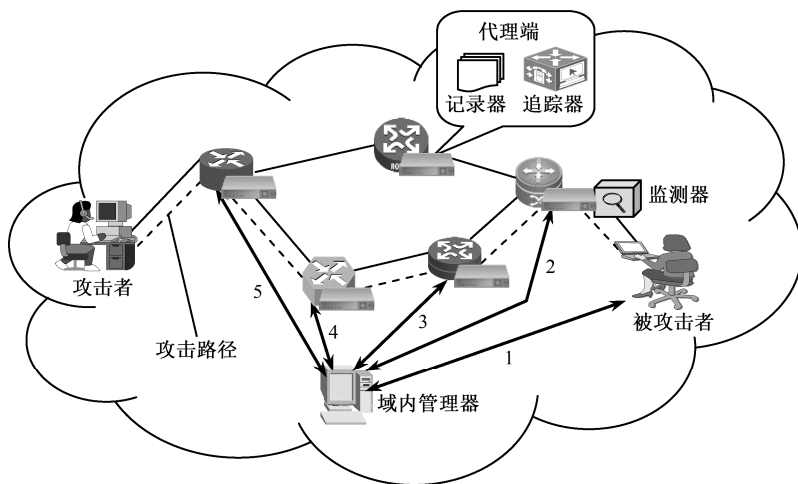


图 8-12 追踪系统及其功能部件

追踪系统的功能部件主要有监测器、记录器、域内管理器和追踪器。

(1) 监测器。监测器被部署在监测节点上，检测网络上的数据包，用来确定是否发生了网络攻击行为，监测器可以是入侵检测系统、防火墙等模块，其实现方式可以是硬件模块，也可以是软件系统。

(2) 记录器。部署在监测节点和转发节点上，记录器的主要功能是往节点内部记录和写入攻击信息。这一部分实现的难点在于数据结构及其算法。

(3) 追踪器。部署在监测节点和转发节点上，追踪器具体实施追踪过程。但是追踪器并不会主动实施追踪过程，追踪器响应追踪命令，并根据追踪命令实施追踪。追踪器工作的基础就是以向量结构形式存储节点记录。

(4) 域内管理器。部署在一台单独的计算机上，域内管理器响应监测器的请求，控制追踪器并管理整个追踪过程。域内管理器是系统追踪系统的中央控制系统，但是这并不说明域内管理器在整个追踪系统中只有一个，实际上域内管理器是一个局部的中央控制系统，一个域内管理器的作用范围根据不同的实际情况大小不同。但是在域内管理器的作用范围内的一切追踪活动都在其控制之下。域内管理器采用分布式结构，在每个自治管理网络内都部署一个域内管理器。若攻击源在一个自治管理网络内，则整个追踪过程由这个自治管理网络内的域内管理器控制；若攻击源的范围超过一个自治管理网络，则整个追踪过程由第一个发出追踪命令的域内管理器控制，由其他域内管理器协助。

(5) 代理端。代理端并不是追踪系统的一个部件，实际上考虑在系统的具体实现上，将记录器、追踪器两个系统部件集成到一起，实现为一个代理端可以简化系统，使系统的部署更加简单。因此，将记录器、追踪器两个部件的集成称为一个代理端。

上面这些部件是追踪系统实际存在的功能模块，在以上部件的具体实现上，代理端可以是转发节点上的一个软件功能，也可以是一个独立的与转发节点相连的硬件模块。域内管理器在实现上可以是一个软件系统。

#### 4. 网络监测器

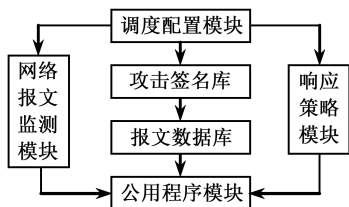


图 8-13 网络监测器的软件模块

位于监测节点上的网络监测器负责监测该网段的数据报文，将收集的数据采样、过滤并将攻击信息发送到管理器。其重要特点是它们的存在对网段中的其他工作站和服务器的透明，不影响正常信息的传输，对网络流量影响极小，仅向管理器发送少量的报警报文。网络监测器的软件模块如图 8-13 所示。

(1) 调度配置模块。设置网络监测器的工作参数，控制网络监测器的工作流程，即从网络中截取报文，送攻击签名库分析，将报文加入报文数据库。如果检测到攻击，则根据响应策略模块执行相应的响应策略（如发送报警信息）。

(2) 网络报文监测模块。以“混杂”方式获取网络的报文，根据不同协议对报文进行解析，然后交由公用程序模块做进一步的处理。

(3) 响应策略模块。包括一个响应策略库和若干响应策略函数。每条响应策略表示：“如果检测到这一种（或一类）攻击，应当采取哪些策略。”响应策略根据其攻击类型描述的具体程度定义优先级，即攻击类型描述得越具体，其响应策略优先级越高。

(4) 攻击签名库。以一定的数据结构分类存储了各种攻击的检测方法，用以对收到的报文进行分析，判断是否为攻击，并返回判断结果以及威胁等级的结构。对于某些具有时间相关性的攻击手段，需要使用报文数据库。

(5) 报文数据库。存储一定时间内收到的报文，用以进行相关性分析。

(6) 公用程序模块。提供了基本的报文解析、内存管理等函数，供其他各个模块调用。监测过程首先由调度模块做一些初始化工作（设置网卡工作方式、初始化系统参数等），然后进入监测过程，开始检测。在检测中，一旦网卡捕获到 IP 报文，就对该报文进行解析，然后根据报文的类型，与各种可能的攻击特征比较。如果发现是攻击报文，则从响应策略库查找相应的响应策略，根据策略采取各种措施，如发送报警信息等；否则，等待下一个报文的到达。

### 8.2.3 网络空间进攻源追踪的系统原理

进攻源追踪就是在网络上有进攻发生后或在数据传输的过程中采取有效的技术措施，去发现进攻源的真实位置和进攻数据在网络中传输的路径的一个过程。下面分别从单自治域和多自治域两种情况下介绍进攻源追踪的原理。

#### 1. 单自治域内进攻源追踪的原理

单自治域内进攻源追踪的系统原理示意图如图 8-14 所示，设该图为网络拓扑的一部



分, 其中  $H_i$  ( $i \in [1, 7]$ ) 为终端主机,  $R_j$  ( $j \in [1, 13]$ ) 为转发节点 (如路由器),  $H_2$ 、 $H_4$  为两个攻击者,  $H_7$  为被攻击的主机。转发节点记录下网上传输的报文信息, 然后在追踪时利用这些记录下的信息, 从与被攻击主机连接的转发节点开始逐跳地追踪到网络攻击源。在转发节点对报文进行转发的过程中每个报文信息被记录在了转发节点中, 这些信息可用来进行报文追踪。

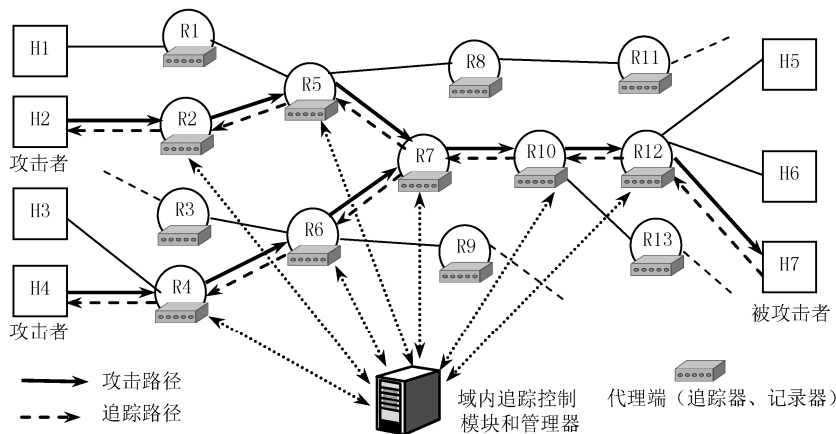


图 8-14 单自治域内进攻源追踪的系统原理示意图

单一进攻源的情况下, 设  $H_2$  为攻击者, 攻击  $H_7$ 。进攻源追踪就是要采用一定技术发现攻击源为  $H_2$ , 同时找到  $H_2$  在进攻  $H_7$  时在网络中穿行的线路为 ( $H_2 \rightarrow R_2 \rightarrow R_5 \rightarrow R_7 \rightarrow R_{10} \rightarrow R_{12} \rightarrow H_7$ )。当位于  $H_7$  相邻代理端的追踪器检测到一次网络攻击, 它将产生一个包含攻击数据报信息的请求给域内追踪控制模块或管理器。如果只查询一个攻击报文, 对攻击路径的表达肯定不充分, 因此, 需要查询多个攻击报文信息。在系统具体实现中, 可以在这里设置一个系统参数来表示需要查询的次数。

在多个进攻源的情况下, 设  $H_2$ 、 $H_4$  为两个进攻者, 进攻  $H_7$ , 进攻源追踪就是要发现多个进攻源, 分别是  $H_2$ 、 $H_4$ , 并且它们在攻击  $H_7$  时在网络中穿行的线路分别为 ( $H_2 \rightarrow R_2 \rightarrow R_5 \rightarrow R_7 \rightarrow R_{10} \rightarrow R_{12} \rightarrow H_7$ )、( $H_4 \rightarrow R_4 \rightarrow R_6 \rightarrow R_7 \rightarrow R_{10} \rightarrow R_{12} \rightarrow H_7$ ), 有更多进攻源时情况类似。

虽然普通网络攻击者可以比较容易地伪造一个数据报的 IP 源地址字段, 但是对于一个数据报的发送者却较难改变数据报经过一系列中间转发节点这一事实。而追踪系统就是要找出数据报经过了哪些转发节点才到达被攻击者的。转发节点记录下这些路由信息, 当回应攻击者的访问请求时, 系统对返回的数据包进行处理, 在数据包中添加特殊的标记, 然后才发送给攻击者。同时通知分布在大大小小各个网络中的代理端, 要求它们开始对数据进行分析, 筛选出带特殊标记的数据包, 并把详细信息发送给追踪控制模块。接下来由控制模块对发送过来的数据进行分析处理, 输出攻击者的真实地址或攻击者最后出现的网络边界地址。具体细节描述如下:

(1) 网络监测器检测到有攻击行为发生, 发出查询请求。一个查询请求由查询序号、

时间值和攻击报文的特征报文段三个部分组成。

(2) 域内追踪控制模块和管理器命令自己管辖的追踪器（位于代理端上）追踪攻击报文。这个命令的结构和前面的监测器发送的查询请求的结构基本相似，只不过将查询序号变成了命令序号用以区分不同的命令。追踪器的追踪过程实际上就是一个查询过程，就是在代理端的节点记录中查询攻击报文是否在其中。查询过程如下：

① 第一步就是分解域内追踪控制模块和管理器发送来的查询命令，分别取出命令序号、时间值和攻击报文的特征报文段。

② 第二步用时间值定位过滤向量，若成功则查询继续，否则，说明查询命令包含的攻击报文的攻击时间不在代理端节点记录中，本次查询完成，查询无结果。

③ 第三步对特征报文段进行  $k$  次哈希运算，若相应过滤向量中的这  $k$  个位置的值都为 1，则查询成功，说明攻击报文经过了代理端所在的转发节点。若  $k$  个位置中有任何一个为 0 或多个位置为 0，则说明攻击报文没有经过代理端所在的转发节点。本次查询命令执行完毕。不管攻击报文是否经过代理端所在的转发节点，都会将查询结果返回给域内追踪控制模块和管理器。

④ 第四步域内追踪控制模块和管理器收到前面的代理端发来的查询结果，根据结果进行下一步操作，若从前面的代理端获得了肯定的答复，继续在域内执行查询命令，重复上面的步骤，直到得到一个局部的攻击路径。如果从前面的代理端获得了否定的答复，那么将重新开始查询其他的攻击报文。

如果攻击报文来自域内，则重复上面的过程就可以找到攻击源的位置。

进行网络源追踪需要整个网络中的所有主机相互配合，通过收集分析网络中的每台主机的有关信息，将进攻者的活动轨迹展现出来。要实现这样的操作，就需要网络中的所有主机都是安全可信的，即网络中的主机没有被进攻者攻击破坏，收集到的数据是可信的，而且在传输这些数据时也没有被破坏或修改，在此基础上对这些收集到的数据进行处理、过滤和筛选，将进攻者在整个网络中的活动轨迹连接起来，实现网络进攻的跟踪。

## 2. 多个自治域之间的进攻源追踪的原理

当攻击者和被攻击者位于不同的自治域内时，追踪过程需要多个域内追踪控制模块和管理器之间进行协调工作，此时这个追踪流程描述如下：

(1) 追踪的开始部分和同一个自治域内的追踪过程一样，直到某个追踪器返回的结果跨越了此自治域的边界。

(2) 此时，这个追踪过程被发起追踪的自治域的域追踪控制模块和管理器提交给相关的自治域的追踪控制模块和管理器继续管理追踪过程。

(3) 每一个自治域中的域内追踪控制模块和管理器在自己的管辖范围内对攻击报文进行追踪并且返回结果给发起追踪过程的最初的那个域内追踪控制模块和管理器。

(4) 最后一个域内追踪控制模块和管理器返回追踪结果给最初的那个域内追踪控制模块和管理器。追踪过程结束。

## 8.3 网络空间进攻源追踪的体系结构

网络空间进攻源追踪的体系结构包括一组部件以及部件之间的联系，是新一代网络攻击源追踪系统的骨架和神经，是首先要研究的问题。下面介绍追踪系统的体系结构。

### 8.3.1 分布式和集中式拓扑结构

为了实现进攻源的追踪，都会在网络拓扑结构上有一些特定的要求。总体来说，也就两种传统的系统结构：分布式拓扑结构和集中式拓扑结构。

#### 1. 分布式拓扑结构

这种体系结构主要是 IP 追踪这类方法所使用，其主要特点是：中间传输节点参与追踪过程，要求中间节点不仅具有数据传输功能，还要能够为进攻源追踪提供服务。在中间节点的帮助下，被攻击的主机能够有效地发现进攻源以及攻击路径，其分布式拓扑结构如图 8-15 所示。

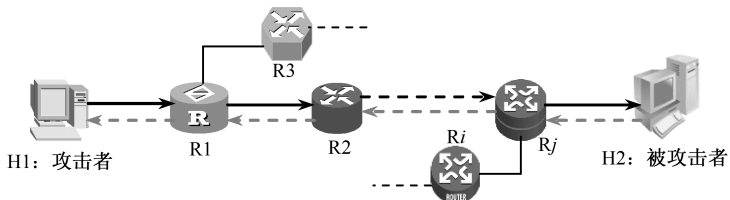


图 8-15 分布式拓扑结构

这个拓扑结构中 H1 为攻击者，H2 为被攻击者，在中间节点的帮助下，H2 发现攻击源和攻击路径，图 8-15 中的攻击路径为： $H1 \rightarrow R1 \rightarrow R2 \rightarrow \dots \rightarrow Rj \rightarrow H2$ 。

#### 2. 集中式拓扑结构

这种拓扑结构主要特点是：在网络的合适位置安插代理或嗅探器，把网络连成一个整体，不仅能够进行攻击检测和追踪，还可以加入响应功能，对攻击行为进行拦截和反击。这些代理或嗅探器把收集到的信息发送给一个分析服务器，由这个服务器来分析这些消息之间的关系，找出哪个主机被入侵，攻击源和攻击路径分别是什么？集中式拓扑结构如图 8-16 所示。进一步，如果这些代理或嗅探器互相之间可以通过协助和通信来完成追踪和响应动作，这样就可以是一个分布式的并且不需要原来中间节点参与的追踪系统。

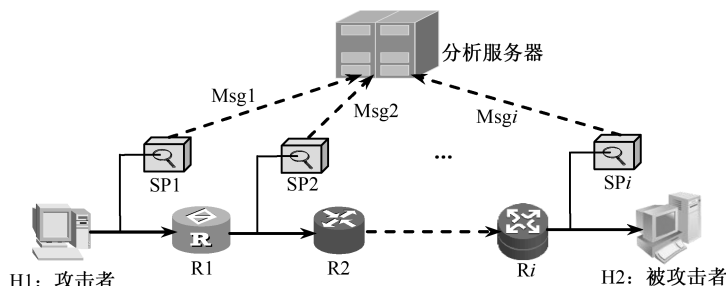


图 8-16 集中式拓扑结构

在这个拓扑结构中，H1 为攻击者，H2 为被攻击者，R1,R2,...,Ri 为中间传输节点，SP1,SP2,...,SPi 为在网络中安插的嗅探器和代理。嗅探器和代理将网络流量信息以消息的形式传给分析服务器，分析服务器通过分析这些消息来找出攻击源和攻击路径。图 8-16 的攻击路径为（H1→R1→R2→...→Ri→H2）。

分布式的拓扑结构借助已有传输设备的计算能力来实现，而集中式的体系结构则是依靠外加具有检测功能的设备来实现，两种拓扑结构虽然在形式上不同，但进行追踪的处理模式都是分布式的检测，集中式的处理，在实现方式上有各自的特点。

### 8.3.2 一种通用网络追踪技术框架

结合作与非作追踪原理，一种通用的网络追踪技术框架如图 8-17 所示。这种框架由协作网域追踪、非协作网域追踪、追踪控制系统和追踪知识系统组成。

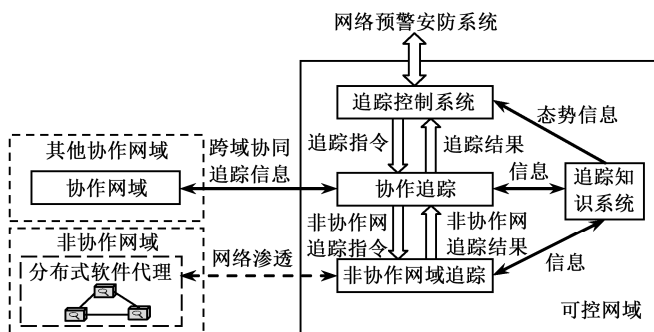


图 8-17 一种通用的网络追踪技术框架

通过在可控网域部署相应的追踪设备，完成协作网域的追踪任务。一旦追踪到可控网域边界，则根据攻击数据入口信息确定可能的非可控网域，进而采取网络信息主动感知的追踪技术，对非可控网域的攻击路径进行分析重构，从而实现在全球网络空间中的追踪。

协作追踪系统将包含多种网络追踪技术，互为补充。根据具体的攻击行为，智能选取

最优追踪技术及策略完成追踪。

实施非协作网域追踪时,需要考虑网络感知(主动拓扑发现、渗透等)带来的不利影响。网络感知说到底,也是某种程度上的网络攻击行为。因此使用网络主动感知的非协作网域追踪,一方面可能被攻击者察觉而采取更为谨慎的措施反制追踪定位,另一方面还可能因为非可控网域的抵制抗议而牵涉到经济、法律,甚至国家政治、外交等方面的问题。

### 8.3.3 网络空间黑客追踪的系统结构

#### 1. 系统主要功能

黑客追踪系统主要提供自动侦查分析、实时监控报警、远程快速追踪和设定网络陷阱等功能,具体包括:

(1) 自动侦查分析功能。通过对被攻击主机的日志、进程、注册表、邮件、账号、共享、连接、Cookies 及现场网络通信等自动分析,确定攻击来源 IP 地址和采用的攻击手法。提供的分析方法有主机基本进攻痕迹分析、应用服务日志分析、进程深层分析、电子邮件分析和通信实时监控。

(2) 实时监控报警功能。对现场进行守候式监控,当黑客再次来访或攻击时,即时报警,并记下攻击者的 IP 地址和攻击方式。

(3) 远程快速追踪功能。通过植入远程追踪探头,分析攻击发起计算机的类型(肉机/控制机),逐级跟踪直到找到发起攻击的进攻者的真实 IP 地址,并尽可能地获取进攻者的计算机中的信息,如获取目标主机静态信息、获取目标主机动态信息、监听目标主机网络通信、进行主机类型分析和进攻痕迹提取等。

(4) 设定网络陷阱功能。在攻击发生时模拟被攻击的网络服务(如 HTTP、FTP、SMTP 等),并对访问进行记录 and 安全性审查,提取攻击者的地址和采用的手法。

#### 2. 系统组成

黑客追踪系统的结构图如图 8-18 所示,主要由攻击分析探头、侦查分析器、实时监控、远程追踪和控制中心组成。攻击分析探头负责获取和整理日志、进程、网络连接等多种信息;侦查分析器负责整理和分析攻击信息,找出攻击行为留下的痕迹,提取攻击行为采用的手法和攻击源地址;实时监控负责监控目标网络服务的运行,对网络服务的访问进行实时安全性审核,根据警报规则发送进攻警报信息,进行进攻痕迹的安全性分析;远程追踪由一组专用远程追踪探头组成,负责进攻到被追踪的主机,潜伏、监听、收集目标主机的信息;控制中心实现整套系统的管理和控制的功能,接收、分析远程追踪探头发回的数据。

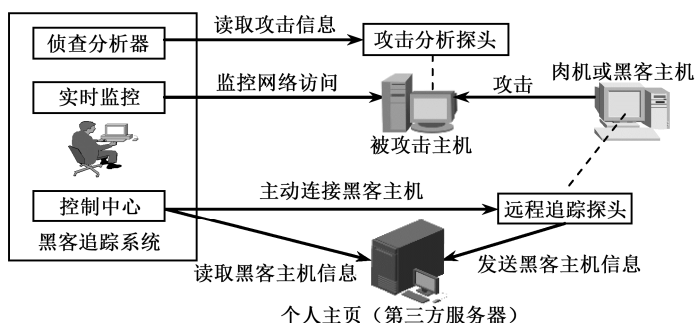


图 8-18 黑客追踪系统的结构图

进行黑客追踪时，首先启动实时监控功能，监控整个网络的服务，控制网络服务的访问，截止和防范黑客的进一步攻击。然后，将攻击分析探头安装到被攻击主机中，收集和整理攻击信息，将信息传送到主系统。接着，使用侦查分析器对这些信息进行深度整理和分析，提取攻击特征和规则，确定黑客的攻击行为和方式。掌握了黑客的攻击信息后，可以对其投放远程追踪探头，入侵黑客的主机系统，潜伏、监听、收集黑客主机的信息和电子证据，并将关键信息和证据返回给控制中心。

### 3. 主要模块说明

#### 1) 攻击信息收集和提取模块

本模块通过扫描系统的注册表、系统进程、系统文件、日志文件，收集、抽取和整理出攻击相关的信息。系统中的文件会备份起来，经过初步抽取和整理的信息保存在数据库中，供系统其他模块使用，以及进行深度的整理、抽取和分析。

#### 2) 攻击特征的分析解码模块

本模块利用网络安全、入侵检测、数据分析等方面的技术，对收集到的攻击信息进行深度的抽取和分析，获得入侵痕迹、攻击源 IP 地址、攻击源类型（肉机或控制机）、攻击发起时间、攻击效果、攻击类型、危害程度等攻击特征信息，作为追踪黑客的依据，同时，产生部分数据证据。本模块的分析技术采用插件的方式根据情况的需求能动态地加入系统中，具有较好的扩展性和灵活性。

#### 3) 信息监听模块

本模块监视目标服务的日志系统，监听目标服务的网络通信，获取对目标服务的访问请求，包括访问请求的方法、URL 资源、URL 查询等，捕获系统消息和网络服务访问请求，截获、拆开、分析和重组数据包。

#### 4) 远程追踪模块

本模块运行在控制中心，用于控制远程主机中的追踪探头，接收追踪探头发送的各种数据。在需要时可对数据进行分析，提取非法的信息，依据分析结果进一步控制远程主机

的网络访问。

#### 4. 远程追踪探头的投放和隐藏

系统利用目标主机中的各种系统漏洞,采用邮件诱骗、进程注入和二次载入等多种方法,将专用远程追踪探头自动投放到目标主机,隐藏于正常系统程序的二进制代码中。为了逃避防火墙对连入本机的连接进行非常严格的检测和过滤,远程追踪探头利用端口反弹技术,通过主动端口连接有固定 IP 的第三方 FTP 服务器或个人主页,将目标主机的信息存于此服务器,控制台通过访问此服务器获取目标主机的信息,然后主动连接客户端。为了更好地穿透防火墙,系统结合 HTTP 隧道技术,将要传输的数据利用 HTTP 协议进行封装,以伪装成 HTTP 数据包,同时把请求的目的端口设置成 80,这样防火墙检测时就认为是安全的数据包,从而在信息探头和分析控制器之间利用 HTTP 协议封装建立起一条安全传输隧道。

### 8.3.4 网络空间多源追踪系统架构

多种追踪技术的融合,主要涉及系统架构设计、追踪信息的规范化、多源信息的有效处理等方面。系统架构需要考虑组件的分布模型、单手段追踪组件的聚合、组件间通信机制等问题,要求能够灵活扩展。追踪信息的规范化是多源信息融合的基础,主要解决统一描述的问题。多源信息的有效处理,涉及来源于不同追踪机制的追踪信息的汇聚、分析、挖掘、判别。系统架构是多源追踪系统的核心技术,是灵活融合多种追踪手段的基础。

基于数据融合的多源追踪系统架构如图 8-19 所示。

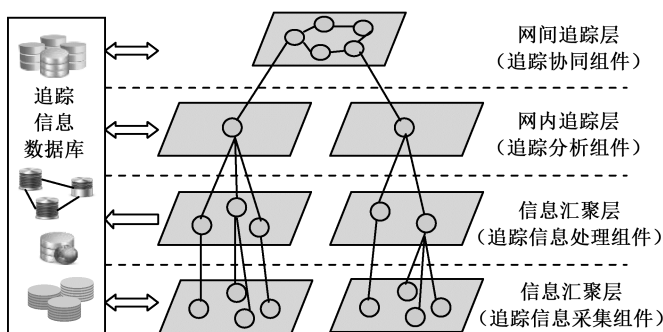


图 8-19 多源追踪系统架构

多源追踪系统由追踪信息采集组件、追踪信息处理组件、追踪信息数据库、追踪分析组件、追踪协同组件等组成。

追踪信息采集组件负责生成、收集、汇聚各种追踪可以利用的信息,具有多种功能各异的形态,如部署于主机的监控软件,收集防火墙、IDS、安全审计系统等日志的信息采

集软件，与综合安全管理系统交互获取安全事件信息的软件模块或设备，路由器内部功能模块（生成 iTrace 及包标记方法的标记等），采集网络数据流信息的专用硬件设备等。

追踪信息处理组件负责汇聚各类追踪信息，通过数据格式转换完成数据规范化后，存储到追踪信息数据库。追踪信息处理组件还实现与单一追踪方法的衔接功能。

追踪信息数据库负责存储追踪信息，但不是一个单独的实体，本身根据网络管理和规模分布，以保证符合管理要求和性能要求。

追踪分析组件处理追踪任务要求，分析查询追踪信息数据库，获得阶段追踪成果，并将跨网络的追踪请求转追踪协同组件处理。

追踪协同组件负责处理跨网络的追踪任务，可按网络管理和规模组织为多个层级，管理域内部可以有更开放的信息互通，管理域之间则需要兼顾追踪任务完成和网络内部信息的保护。同时，追踪协调组件还负责集成跨网络追踪方法，如基于 DNS 的攻击追踪等。

多源追踪的核心即多种追踪方法的有机融合，通过追踪分析组件和追踪协同组件实现，处理不同追踪方法之间的特征数据变换、关联分析和过程的衔接。

追踪信息来源较多，包含多种不同类型的追踪信息，如安全事件信息、网络数据包信息，信息的保真度也有差异，如基于网络数据流日志的追踪，有的包含完整的数据包信息，有的只包含数据包的摘要信息。因此追踪信息的处理较为复杂，涉及追踪信息的规范化、网络数据包特征信息变换、追踪信息的关联分析等。下面以一个简化的场景（即多源攻击归因示范如图 8-20 所示）说明其工作原理。

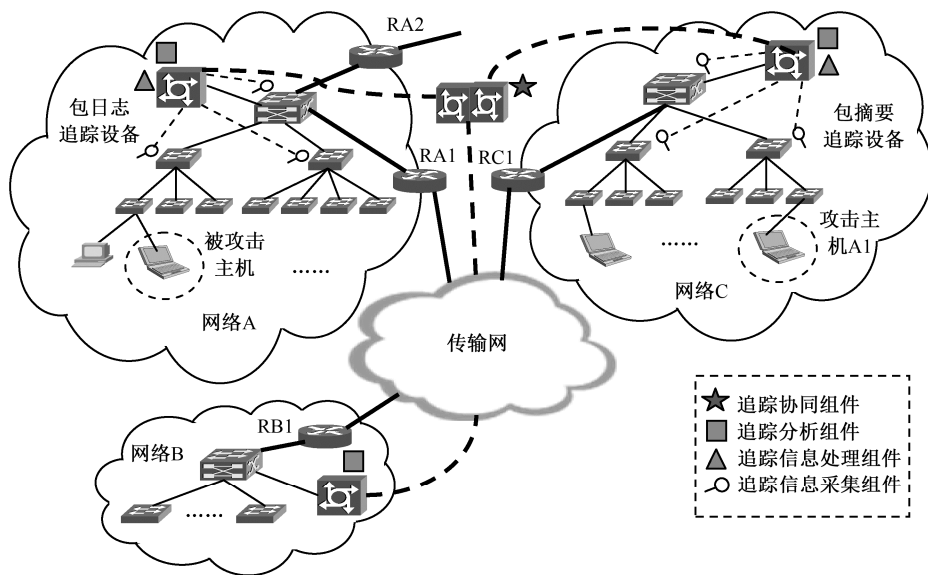


图 8-20 多源攻击归因示范

网络 A 发现一个攻击包，将攻击包完整信息提交追踪系统；网络 A 部署有包日志采集设施，并保存了完整包信息；网络 A 追踪分析组件查询内部数据库（根据网络 A 规模可集中保存，也可分布式存储），确定攻击来源于网络 A 外部，并确认来自边界路由器 RA1；网络 A 追踪子系统因此将追踪任务交域间追踪子系统进行进一步追踪；若域间追踪子系统



(追踪协同组件)支持基于 sFlow 等协议的追踪,可确认攻击来源网络 C,则交网络 C 进一步追踪;如果没有相关机制支持,也可根据路由器临近关系,将追踪任务包括攻击包数据交临近网络 B、C 等的追踪子系统处理;网络 C 追踪子系统部署了基于包摘要的追踪设施,先根据攻击包数据计算摘要和内部数据库中包摘要记录对比,根据记录匹配确定攻击主机 A1 及 A1 与边界路由器 RC1 之间的路径;如果攻击主机 A1 部署了安全审计设施,则提取相关日志记录,否则根据 A1 的网络流时间、流量等特征,分析判断 A1 是否只是被攻击者利用的僵尸机或跳板;如确认是攻击控制主机则结束追踪过程并将追踪结果返回,否则提取攻击的上一跳追踪信息进一步追踪攻击者。

多源追踪的架构具有以下特性:

- (1) 松耦合。以追踪信息为中心融合不同追踪方法,减轻了过程结合的强耦合问题。
- (2) 易部署。可分阶段部署追踪系统,系统允许部分部署时完成可追踪部分路径的追踪,可以在缺少部分中间环节时完成追踪。
- (3) 扩展性。容易集成不同追踪机制的底层设施,便于增加新的追踪机制。
- (4) 分布式。追踪信息存储和处理均分布于网络,降低单点处理能力要求,强化系统及时响应的能力。

### 8.3.5 网络空间主动追踪机制体系结构

网络空间主动追踪机制是通过分布在网络各个合适位置的代理,把网络连接成一个整体,不仅能够进行攻击检测和追踪,还可以加入响应功能,对攻击行为进行拦截和反击。这些代理互相之间通过协助和通信来完成追踪和响应动作。

网络空间主动追踪机制可以描述如下:安全追踪设备发现自治域内的主机被入侵,启动追踪过程向所有相邻的安全追踪设备发送追踪消息,等待返回结果。一个安全追踪设备接到一个追踪消息后,首先判断一定时间段内是否接收过与这个追踪消息的关键内容一致的消息,如果收到过类似消息,追踪过程在这个安全追踪设备上就终止了;否则,就搜索本身监测到的入侵信息,进行相关性分析。如果没有发现相关的入侵事件,这个安全追踪设备就终止追踪过程;否则,继续这个追踪过程。

要实现这种机制,在网络拓扑上要有自己的结构,安全追踪设备自身的实现机制也要有层次结构。

#### 1. 主动追踪机制拓扑结构

网络空间主动追踪机制所具有的体系结构从拓扑结构上看也是分布式的,但与前面所介绍的分布式拓扑结构不同的是:实现主动追踪机制拓扑结构分布式的是安全追踪设备而不是中间传输设备。主动追踪机制的拓扑结构如图 8-21 所示。

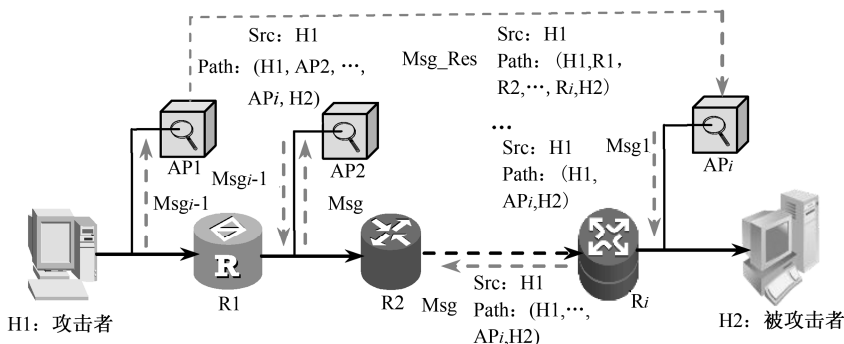


图 8-21 主动追踪机制的拓扑结构

这个体系结构中，H1 为攻击者，H2 为被攻击者，R1,R2,...,Ri 为中间传输节点，AP1,AP2,...,APi 为在网络中安插的安全追踪设备，APi 发现自己与主机被攻击，把攻击信息通过信息以消息的形式传递给相邻安全追踪设备，在攻击路径上的安全追踪设备分析这些消息来找出攻击源和攻击路径，最后将追踪结果返回给发起追踪的安全追踪设备，如图 8-21 中 Src: H1; Path: H1→R1→R2→...→Ri→H2。

## 2. 安全追踪设备体系结构

安全追踪设备是实现主动追踪机制的基础。大部分的计算、分析和传输都在安全追踪设备上完成。安全追踪设备由监测层、分析层、消息层和数据流组成，其实意图如图 8-22 所示。

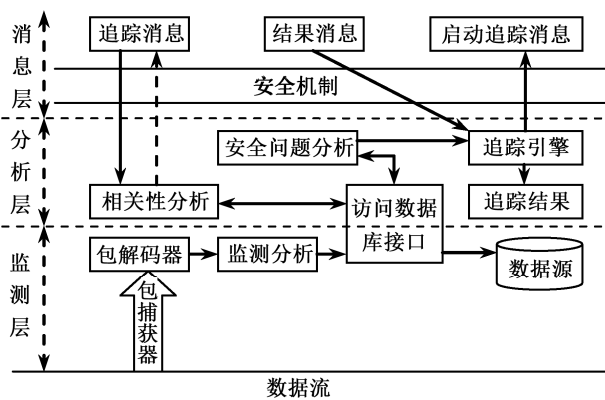


图 8-22 安全追踪设备体系结构示意图

监测层是主动追踪过程的基础和起点，主要包括包捕获器、包解码器、监测分析模块和数据输出。监测层完成的主要功能有：

(1) 捕获数据包。捕获数据包由包捕获器完成，为分析和发现攻击提供数据，这里的捕获并不是拦截，仅仅是把流经安全追踪设备的数据包复制一份传往下一个处理步骤，并且尽可能多地捕获数据包，这样加大发现攻击信息的概率和准确性。

(2) 分析数据包信息。接收捕获的数据包后，由包解码器对数据包进行解码分析，主要对包头信息和短数据包的内容信息进行提取和规范化，提高监测分析的准确性。

(3) 发现攻击信息。这是监测层最核心的工作，在得到的数据包信息中，按照一定的方法进行监测分析，力争发现攻击信息。

(4) 输出攻击监测结果。如果发现安全问题，就把结果输出到数据库中，为后续进行主动追踪提供数据源。

分析层主要完成主动追踪的计算、消息处理等工作，是整个追踪机制的核心部分，分析层完成的主要功能有：

(1) 提取攻击信息。主要是从数据库中提取已经发现的针对本域内主机的攻击信息，还可以对这些攻击信息进行简单的融合，形成最终的攻击信息报告，把这个报告提交给追踪引擎，让追踪引擎启动追踪过程。

(2) 启动追踪过程。追踪引擎接到攻击信息报告后，启动追踪过程。追踪引擎向相邻的安全追踪设备发送追踪消息，同时为启动的每一个追踪过程建立唯一的一个标志和定时器，等待接收返回消息。

(3) 进行相关性分析。这个过程是在接收到相邻安全追踪设备的追踪消息之后启动，首先记录该条消息的内容，再查看攻击信息数据库，进行相关性分析。如果发现有相关攻击信息，就把自身地址加入消息中，发送给除了消息来源地址以外的所有相邻安全追踪设备；否则就停止在本设备上的追踪。

(4) 输出追踪结果。安全追踪设备在接到自己发起的追踪过程的返回消息时，把这个消息输入数据库或在显示设备上显示。

消息层负责消息的形成、发送和接收，消息是连接各个节点和进行追踪的信息纽带。消息层主要工作有实现通信的安全机制、发送启动追踪消息、发送和接收追踪消息和接收结果消息。

数据流是整个主动追踪过程处理的主要数据对象。它的主要功能有：

(1) 配置和存储相邻安全追踪设备地址信息。这些信息是追踪能够进行下去的保障，并且会随着拓扑结构的变化而随之变化。

(2) 配置和存储安全追踪设备所在域内的地址范围信息。这些地址范围原则上是受保护的，同时也是找到攻击源的信息依据，这些信息也会随时变化。

(3) 维护数据库信息。这些信息包括由监测层输出的攻击信息、收到的攻击追踪信息和收到的攻击追踪结果信息等，其中攻击信息和攻击追踪信息都会随时间更新，一段时间之后淘汰存在时间较长的一些信息，以保证在进行分析时效率较高。

## 8.4 网络空间 IP 源追踪技术

在网络中，任意两台终端要进行信息的沟通与数据的交换，其间必定会建立一条或长或短的通道（又称“路由”），每一条路由都必定经过多个节点和多条链路。在基于 TCP/IP 协议的网络中，终端之间的通信是通过 IP 报文传递来实现的，路由的建立则是基于 IP 报文中的 IP 地址。因此，IP 追踪技术的基本思想通常是：通过路由节点的帮助回溯出包经过的路径或包的源地址，要么让 IP 报文记录下所经路由节点的信息，要么让路由节点记录下 IP 报文的信息，或者二者均记录。

IP 追踪所面临的情况主要有以下几种：第一种，也是通常的状况，所传输的 IP 报文中的源 IP 地址是真实的 IP 地址，它与网络行为发起者也是直接关联的。第二种情况是，网络行为者伪造了 IP 报文中的源 IP 地址。第三种，网络攻击者通过某种中间“跳板”来隐藏自身的行踪。针对这些问题人们提出了一些解决方法：一类称作 IP 源追踪技术，目的是识别发送 IP 报文的真实的源 IP 地址，该类技术主要是在一系列路由和网关的帮助下在网络层执行。另一类称作跨越“跳板”的追踪技术，目的是识别通过“跳板”隐藏身份的真正攻击源，目前主要有 Thumbprint 方法、TCP 序列号分析法等。

IP 源追踪技术可分成两类：主动式追踪和被动式追踪。主动式追踪能够在转发数据包的同时进行实时监测，当攻击发生时可根据监测结果重构攻击路径。主动式追踪技术包括数据包标记、路由记录和 ICMP 消息等。被动式追踪在检测到攻击后才开始引发追踪过程，这就要求必须在攻击尚未结束时完成追踪，否则一旦攻击停止，追踪过程就会失败，如入口过滤、链路测试和层叠网络追踪等。

### 8.4.1 数据包标记法

数据包标记法是确定网络攻击与入侵的基本方法，主要思想是在网络中的路由器选择转发的数据包包头的某些特定字段当作标记空间，并向这个标记空间中写入某些状态信息，如路由器信息或者链路信息。被攻击者收到这些带有标记信息的数据包后，进行状态信息的汇总和分析，最终得到完整的攻击或入侵数据包在网络中的传输路径。

用数据包标记法来进行网络追踪在现实中存在一些困难。首先，要求数据包捕获主机具备记录大量数据包的处理和存储能力；其次，数据包中没有足够的空间来记录完整的路径序列；第三，路由器向每一个转发的数据包添加数据将导致路由器开销较高；第四，要求数据包捕获主机并有进行自动分析的能力，面对经过关键路由器的海量网络数据，手工分析是绝无可能的；第五，攻击者可以通过伪造数据包来逃避追踪；第六对数据包进行保

存、记录和共享，将会涉及隐私与法律问题。为了解决这些问题，提出了概率性数据包标记法和确定性数据包标记法。

1. 概率性数据包标记 (PPM) 法

PPM 法的主要思想是路由器在转发报文时按照一定的概率有选择地将标志信息写入转发的数据报文头部中，当被攻击主机收到足够的数据包后就可以根据样本数量排序重构出攻击路径，对攻击者进行 IP 回溯，发现攻击源。

如果一个路由器决定去标记一个经过的数据包，会把它和它的下一跳路由器之间的路径信息写入到数据包的包头中。首先把自己的 32 bit 的 IP 地址写入到数据包的 IP 包头中，当作是链路起始地址，并且将距离域置为 0。它的下一跳路由器，如果要标记该数据包，则会覆盖之前的链路起始地址，并且将距离域置为 0；如果不是要标记该数据包并且数据包中距离域为 0 的话，就会将其 IP 地址写入到链路结束地址，并且将距离域的值加 1；如果不标记该数据包而且数据包中的距离域也不为 0，则只是将距离域加 1。由于数据包在网络中的传输跳数一般都小于 25 跳，因此用 5 bit 表示数据包在网络中的传输距离。概率性数据包标记法的标记域的空间结构如图 8-23 所示。

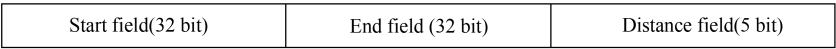


图 8-23 PPM 法的标记域的空间结构

一般情况下，描述一条链路的相关信息所需要的空间会大于数据包 IP 包头 Identification 字段所能提供的 16 bit 的空间，该方法用分片的方法解决这个问题，也就是多个数据包共同承载同一条路径信息。概率性数据包标记中对于 Identification 字段的使用方案如图 8-24 所示。

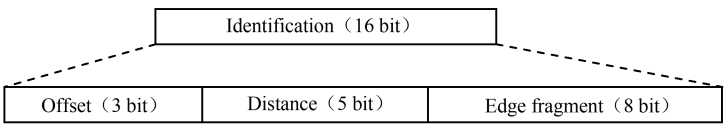


图 8-24 概率性数据包标记中空间使用方案

PPM 法将一条链路的标志，即起始和结束路由器的 IP 地址，分成 8 片，每片包含 8 bit，并且使用 3 bit 指示分片的位置，另外使用 5 bit 存储数据包在网络中传输的距离信息。该方法采用固定的标记概率，概率值为可能传输的最大路径的倒数，即 1/25。在被攻击端，收集到一定数量的数据包后，根据距离域的不同值将地址分片进行拼合，得到完整的 IP 地址，最终得到数据包在网络中的传输路径。

该方法需路由器提供额外的支持，不审计流经路由器的所有流量，而是按一定频率对报文流进行采样。该方法不适合追踪流量小的攻击，只适合追踪产生大流量的攻击。有关概率性数据包标记法的实现，人们提出了节点附加、节点采样概率包标记、边采样概率包标记、压缩的边分片采样概率包标记、高级包标记、认证包标记、下一节点验证概率包标

记和动态概率包标记等方法。下面对这几种方法进行简要分析。

### 1) 节点附加法

数据包标记的最简单实现方法是节点附加（Node Append）法，即在 IP 头的选项字段中将路由信息完全标记到数据包中，节点附加法原理图如图 8-25 所示。其核心思想是：当数据包经过路由器转发时，路由器将自己的 IP 地址标记到数据包中的适当位置，如 IPv4 中的选项域（Option）。

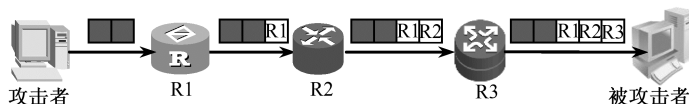


图 8-25 节点附加法原理图

节点附加法收敛速度很快，并且被攻击者只需收到一个攻击包就可重构出攻击路径。但它仍存在多方面的局限性使其不太可行。首先，由数据包的发送方到接收方之间的距离是未知的，因此在数据包中将会标记多少路由信息也就未知，过长的路由信息可能会导致某些数据包路由信息长度超过路径的最大传输单元（MTU，Maximum Transmission Unit），而产生不必要的分片；其次，节点信息的附加操作是很耗时的，并且会明显增大路由器开销，进而影响网络的性能和某些应用。因此，要在数据包中标记完整的路由信息是不太可行的。

### 2) 节点采样概率包标记法

节点采样概率标记法在 IP 报文头里预留一个 4 字节的“节点域”，当路由器转发报文时，都以概率  $P$  将自己 IP 地址写入该域。设报文从路由器到目的地要经过  $d$  跳，则目的地收到该路由器以概率  $P$  标记过的报文的概率为  $P(1-P)^{d-1}$ ，它是一个严格递减函数，因而在目的地收到的带路由器标记的报文的数量随路由器离目的地距离的增加而减少，这样就可以对收到的带有标记的报文按照不同的标记进行计数，然后按照大小进行排列，就可得到报文的传播路径。

在  $d=15$ ， $P=0.51$  的情况下，被攻击者平均要收到 42 000 个报文，其中才有一个是距离最远的路由器采样过的报文。因而该方法在样本空间必须特别大的情况下才能正常工作，否则将不能确定路由器的先后次序或颠倒先后次序。

这种方法虽然减轻了路由器的负担和网络流量，但是还存在以下缺点：首先，从样本的分布推断出路由器的排列次序是一个很慢的过程；其次，如果采样概率选得过大，距离被攻击者越远的路由器的样本越少；第三，当同时有多条攻击路径时将失去作用；第四，当攻击者伪造数据包中的标记信息，攻击者通过控制攻击路径上的一个节点伪造节点的标记信息时，在被攻击主机上不能判别这些伪造的信息，将导致构造出错误的攻击路径。

### 3) 边采样概率包标记法

在边采样概率包标记法中，路由器向 IP 数据包头中标记的是由一个节点和其下一个

节点所组成的边的信息。该方法要在 IP 首部增加三个域：Start、End 和 Distance 域。其中，Start 和 End 存储“边”信息，Distance 存储被标记的路由器开始所经过的距离。路由器以概率  $P$  对数据包进行标记，如果路由器对数据包进行标记，则把自己的 IP 地址写入 Start 域，同时把 Distance 置 0；如果路由器不对数据包标记，则检查它的 Distance 值，如果为 0，证明上边的路由器对数据包进行了标记，把自己的 IP 地址写入 End 域，与前一跳路由器之间形成一条边。如果不是 0，则只将 Distance 加 1。Start 和 End 构成了链路的一条“边”。被攻击者根据收到的标记包中的信息，通过 Distance 域排序将边信息匹配连接重构出攻击路径。在此方案中，Start 域 32 位，End 域 32 位，Distance 域 5 位（一般数据包所经过的路径不超过 30 跳，故用 5 位即可存放距离信息），共需 69 位来存储路径信息，而数据包的 Option 域只有 16 位，远不能满足需求。

该方法相对减轻了路由器的负担，强制性地增加距离字段是为了减少攻击者的欺骗性。当数据包到达被攻击主机时，距离字段表明了从它所包含的边被取样后转发的跳数。由于攻击者产生的任何数据包中的距离一定比实际攻击路径更小或相同，所以单个的攻击者无法伪造成与被攻击主机之间的任何边，并且被攻击主机在重构攻击路径时也不用担心被欺骗。另外，因为不再使用样本排列方法来区分“虚假”样本，所以可以使用任意的标记概率。被攻击主机通过攻击数据包中记录的边可以构建出一幅能够回溯到攻击源的有向图。因为被攻击主机离路由器越远，其接收到样本的概率就越低，所以此算法的收敛时间取决于从最远路由器收到一个样本的时间。这样，即使有距离相等的节点以相同的概率标记数据包，重构算法并不需要依据接收到的该节点所标记的数据包的个数来判别其相对于被攻击主机的距离，而是通过被标记 IP 数据包中的 Distance 域的值以及边的信息，来重构攻击路径。这样就解决了 DDOS 攻击情况下的攻击路径重构问题。

#### 4) 压缩的边分片采样概率包标记法

边采样概率包标记法为了标记一条边的信息需要占用 69 比特的存储空间，这在 IPv4 的报文头中是无法实现的。为此，提出了压缩的边分片采样概率包标记法来解决 IP 报文头空间不够的问题。该算法对边采样的标记算法进行了三步改进：第一步，通过两个 IP 地址的异或记录“边”信息；第二步，将“边”信息分段；第三步，加入错误检验码。具体方法是：以节点 IP 地址  $A$  为参变量，求解  $B = \text{Hash}(A)$ ，将  $A$  与  $B$  每位交叉，组成一个新的代表该节点扩展的地址信息，将其分段之后，随机选择一段，将其与分段的偏移量填充到 IP 报文头，并设 Distance 字段的值为 0。在后继的节点上，检测到 Distance 值为 0 时，将自己扩展的地址信息进行分段，选取具有同样的偏移量的分段与 IP 报文头中的信息进行异或运算，产生边的信息，将该信息写入报文头中，并将 Distance 值加 1。在被攻击主机上重构攻击路径时，只有一条边的两个节点的 IP 值和 Hash(IP) 值都匹配时的数据包才会被接收。

压缩的边分片采样概率包标记法虽然改进了边采样概率包标记法在 IPv4 的报文头中空间不足的问题，然而却也带来了新的问题。由于在压缩的边分片采样概率包标记法中采用了 Hash 函数，同时将边信息分段处理，因而不可避免地出现了 Hash 冲突以及分段后所

选段冲突问题，造成了大量的虚假攻击路径，同时使得重构算法的计算量急剧增加，在攻击路径重构时间上显得让人难以忍受。

### 5) 高级包标记法

在一般包标记法中，被攻击者重构攻击路径的计算量非常庞大，同时当 DDoS 攻击的分布性很强时，具有很高的误报比率，这种情况下往往会重构出错误的攻击路径。为了改进一般包标记法的不足，人们提出了高级包标记法和带认证的包标记方法。

在高级包标记中，路由器利用 8 个输出各为 8 比特的 Hash 函数  $h_0, h_1, \dots, h_7$ ，来对 IP 地址取 Hash 值。这样数据包里标记的是 IP 地址的 Hash 值。假设当路由器标记一个数据包时，将距离（初始值赋为 0）、IP 地址的某个 Hash 值  $h_i(\text{IP})$ （从 8 个 Hash 值中随机选取）以及对应的 Hash 函数的编号填入标记域中；当路由器不标记一个数据包时，则只将距离域的值加 1。在被攻击者处重构攻击路径时，被攻击者先将得到的 Hash 值按距离、Hash 函数的编号分成不同的集合，设为  $S(d, n)$ ，这里  $d$  表示距离， $n$  表示 Hash 函数的编号， $n=0, 1, \dots, 7$ 。然后将被攻击者作为攻击路径的开头，从距离  $d=0$  开始，对攻击路径上到被攻击者距离为  $d$  的节点（当  $d=0$  时，这样的节点只有被攻击者自身）的每个上游路由器  $R$ ，设其 IP 为  $\text{IPR}$ ，分别求  $h_i(\text{IPR})$ ，如果对于所有的  $n$  从 0 到 7 都有  $h_i(\text{IPR}) \in S(d, n)$ ，则将  $R$  计入攻击路径中到被攻击者距离  $d+1$  处，并将  $R$  与到被攻击者方向的下游路由器的连接记入攻击路径中作为距离被攻击者  $d$  处的一条边（当  $d=0$  时，这个下游路由器指被攻击者自己，而记入攻击的边就是  $R$  到被攻击者之间的连接）。对于  $d=0$  处理完以后，处理  $d=1$  的情况，如此依次处理，直到  $d$  达到可能的最大值而不能继续为止。

高级包标记法与一般包标记法相比，在被攻击者重构攻击路径时所需的计算量少了许多，在分布式攻击下的误报率很少，而且扩展性也更好。但是，在高级包标记法中，路由器往数据包标记的信息是路由器 IP 地址的 Hash 值，而 Hash 函数是单向的，这就使得被攻击者必须知道上游网络的拓扑信息。由于攻击者可能来自互联网上的任何地方，这就意味着被攻击者几乎要预先知道整个互联网的拓扑信息，这是很有难度的，尤其对于小型企业和普通用户而言。同时，网络的拓扑结构处于不断地变化之中，因此用户还必须时刻更新最新的拓扑信息，使得该方案的广泛应用受到限制。

### 6) 认证包标记法

高级包标记法的一个主要缺点是这种标记没有被认证。一旦某个路由器被攻破，高级包标记法就能根据精确的概率分布冒充上游路由器进行包标记，并且能防止被攻击者通过分析包标记的分布来检测和确定被攻破的路由器。为了解决这个问题，采用带认证的标记。

认证包标记法与高级包标记法类似，不同的是路由器标记数据包时还要对标记的内容进行加密以达到认证的目的。在认证包标记法中，每个节点  $i$  首先生成一系列的密钥  $\{K_{j,i}\}$ ，每一个  $K_{j,i}$  都是一个 Hash 函数链中的一个。通过一个单向函数  $g$ （例如 MD5），只能单向向前或向后计算得出密钥链，例如， $K_{j,i} = g(K_{j+1,i})$ 。时间被分割成一段一段的间隔，每个节点  $i$  在某一个时间间隔  $t$  内只使用一个密钥  $K_{t,i}$ 。节点  $i$  使用  $K_{t,i}$  作为密钥计算消息认证



码 (MAC, Message Authentication Code), 并将 MAC 作为标记信息。在时间间隔  $t$  结束后, 再延长一段时间, 保证在节点与被攻击主机间有足够的时间同步, 然后将密钥  $K_{t,i}$  公开。被攻击主机接收到数据包时, 保存每一个数据包的到达时间。在重构攻击路径时, 被攻击主机首先根据接收到的数据包的时间, 根据时间同步方法, 确定节点标记数据包的时间。根据标记时间和节点公布的当前密钥来确定标记时使用的密钥, 就可以解开 MAC 了。

认证包标记发利用 Hash 函数的单向性, 不同的节点以不同的 Hash 函数来计算 MAC, 各个节点之间互相不知道对方所运行的 Hash 函数。假设 A 节点以 Hash(A) 来计算 MAC, 如果 B 以 Hash(B) 来计算 MAC 冒充 A 的标记, 在被攻击主机上运行重构算法时以 Hash(A) 来还原计算的结果的标记就会出现错误, 被攻击主机就会丢弃该被标记的数据包。因此, 该法具有一定的抗干扰能力。

然而, 当一个节点被攻击者控制并用来伪造标记信息时, 虽然重构算法可以排除该节点的伪造信息的干扰, 但它不知道是哪一个节点在伪造信息。而且, 与被控制节点在同一条攻击路径上的距离比被控制节点远的节点, 即使其是正常标记边的信息, 由于被控制节点错误信息的干扰, 那些节点组成的边信息也不能再重构出来。同时, 由于 Hash 函数的单向性, 使得 IP 报文头中标记的边信息不能直接用在重构算法中, 这就需要事先了解整个网络拓扑才能重构出攻击路径。

#### 7) 下一节点验证概率包标记法

在压缩的边分片采样概率包标记法中边信息的标记上, 是在边的起始点标记边的起始信息, 在边的终点标记边的终点信息, 边的起始信息与终点信息是在边的终点通过异或运算写入了同一个域中, 在被攻击主机上再重新恢复节点的标记信息。因此, 在重构算法时, 缺乏边的起始点与终点的相互验证。一旦某一节点被攻击者控制, 就会使得与该节点相连接的边的信息被伪造, 得不到这些边的正确信息。下一节点验证概率包标记法针对此缺陷进行了改进。同时, 该方法重构攻击路径时不需要事先了解整个网络的拓扑。由于一个转发数据包的节点, 很容易得到与它直接相连接的其他节点的地址信息。因此, 该方法中, 标记一条边的起始节点时, 不仅仅标记自身的节点信息, 还把边的终点信息即下一跳节点的信息标记在 IP 数据包头中, 而在下一跳节点即边的终点再把自身的信息标记在另一个域中。这样, 在被攻击主机的重构算法中可以通过两次标记信息的相互验证, 来确定这条边的标记信息是否可靠。

#### 8) 动态概率包标记法

针对压缩的边分片采样概率包标记法和高级包标记法, 人们提出了一些类似的改进方法。其主要思想都是利用 IP 报文头中的生存时间 (TTL, Time to Live) 值动态决定节点标记数据包的概率, 使标记算法和重构算法得到更好的收敛速度和性能。由于固定概率的包标记方案中, 相对于攻击者越近的路由器, 被标记的数据包数量反而越少, 导致被攻击者在路径重构时不能准确地定位攻击者方位, 并造成收敛率的严重下降。所以人们分别提

出了动态概率和自适应概率的包标记方案，旨在提高攻击者附近路由器或边界路由器的标记概率。虽然标记和重构的具体方法以及 IP 报文头字段的重载都没有太大的区别，但是，这些标记方案存在着 TTL 值被伪造的缺陷。

## 2. 确定性包标记 (DPM) 法

概率性数据包标记法所共有的一个局限性是需要分析的攻击包数量比较多，因此只能对大流量的攻击进行追踪。但是现实中还存在着许多小流量的攻击，甚至一个包就可以形成攻击，并且造成的破坏性丝毫不亚于 DDoS。由于 IP 包是网络传输中的最小单位，IP 追踪最理想的情况是能对任意单个 IP 包进行追踪。针对该类问题，提出了非概率的确定性包标记方法。

DPM 在边界路由器对进入自治域的数据包进行确定性标记，每一个支持 DPM 的边界路由器会在转发口对每一个通过它进入网络的数据包进行标记，DPM 使用数据包 IP 包头中的 Identification 域以及 Reserved Flag 共 17 bit 来保存标记信息。与 PPM 不同，DPM 不再存储链路信息，而只是存储路由器节点本身的地址信息。为了能将路由器 32 bit 的 IP 地址标记到数据包中，DPM 将路由器 IP 地址分为两部分，每个部分各为 16 bit。追踪路由器在进行标记时，以 0.5 的概率选择地址分片对数据包进行标记。当选择第一个分片时，将这部分地址信息存储于 Identification 域中，并且置 Reserved Flag 值为 0；同样，当选择第二个分片时，将这部分地址信息存储于 Identification 域中，并且置 Reserved Flag 值为 1。被攻击终端在收集到足够路径信息后，就可以根据特定的路径构造算法得出攻击包的真实源地址。

但是确定性包标记法和前面提到的概率性数据包标记法还是存在很大差异，最重要的有两点：①PPM 需要攻击路径上的所有路由器都参与路径信息的标记，而 DPM 不需要所有路由器都参与数据包的标记，只需要第一个入口边界路由器具有标记路径信息的功能；②PPM 中的路由器对经过的 IP 包以一定的概率进行标记，而 DPM 则是由入口边界路由器对每一个所经过的 IP 都进行标记。

网络攻击追踪的最终目标是找到攻击的发起者，所以 DPM 中对入口地址进行标记的方法，相比较 PPM 中对所有路径进行标记的方法而言，对问题的解决更为简捷有效。该方法克服了 PPM 中路径构造算法复杂、误报率高的缺陷，并且健壮性也有所提高，而且具有追踪小流量攻击和反射攻击的潜力，是一种很具使用价值的追踪技术。但是 DPM 的有效性及其依赖边界路由器支持的范围和强度，这种要求使其离实际应用还有一定的差距。因此，如何增强边界路由器标记的容错性和使其实施方案更具可行性成为当前研究的热点。

### 8.4.2 路由记录法

要追踪攻击源，一种简单直观、最容易想到的方法就是利用路由器的日志功能，对其

所转发的报文进行记录，但是记录会耗用路由器大量的运算资源和存储空间。

利用路由器的日志功能，在检测到攻击后便可以通过查询这些日志来追溯到攻击者。首先需要在关键路由器上记录转发的每个数据包的特征信息和上游路由器的地址，对数据包进行日志登记，随后用数据挖掘技术回溯包的传输路径。路由器运行过程中会向日志主机发送日志。通过登录日志主机，系统管理员可以了解日志事件，对日志进行分析，再采用数据挖掘技术可得到报文传输的路径。

另一种思路就是将数据包经过路径的路由器地址信息写入数据报文中，被攻击者收到攻击数据包后就可以从报文中提取出路径信息，构造出攻击数据的攻击路径，就可以追踪到攻击者，这就是路径记录法。

在 IP 报文头的 IP 选项里有一项路径记录功能，可以用来记录报文从攻击者到被攻击者所经过的路径上的各路由器的 IP 口地址，路径记录法就是利用该功能来记录路径信息。带路径记录选项的 IP 报文结构图如图 8-26 所示。

版本	头长度	服务类型	总长度	
标识			标志	段偏移
生存时间	协议类型		校验和	
源IP地址				
目的IP地址				
选项码	长度		指针	
路径上的第一个路由器的IP地址				
路径上的第二个路由器的IP地址				
.....				
数据				

图 8-26 带路径记录选项的 IP 报文结构图

其中，“选项码”为 7，表示路由器在转发报文时，要将自己的 IP 地址添加到报文中。长度指出 IP 数据报发送主机预先分配给该 IP 地址存储区域的大小，指针指向该存储区域内下一个用于存放 IP 地址的位置。如果预先分配的地址区域大小不足以记录下全部路径，IP 协议将放弃记录余下的地址。

因为数据报文的 IP 选项域也并没有足够的空间存储路由信息，所以出现了另一种思路：用记录 IP 地址信息的摘要来节省存储空间。被攻击者可以根据所收到的攻击数据包的摘要和路由器中保存的摘要重构攻击路径，源路径隔离引擎就是比较成熟方法之一。该方法的优点是能够对单个数据包进行很准确的反向跟踪，漏警率为零，且有很好的互操作性。缺点是它需要 ISP 间的相互合作，对高速路由器存储要求高，并会消耗路由器 CPU 资源，影响路由器的流量转发性能。

## 8.4.3 ICMP 消息法

### 1. ICMP 简介

ICMP 即因特网控制报文协议，是一种特殊用途的报文机制，可以使互联网中的路由器或主机报告差错或提供有关意外情况的信息。

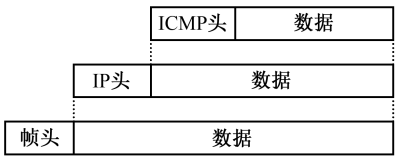


图 8-27 ICMP 报文的封装

ICMP 报文的封装如图 8-27 所示，ICMP 报文放在 IP 数据报的数据部分，IP 数据报则放在帧的数据中进行网络传输。ICMP 报文与其他普通报文一样，具有相同的路由选择，并没有特殊的优先权和增加可靠性。

在 ICMP 头中包含了三个字段：1 字节类型域、1 字节代码域、2 字节校验和。类型域表示了该报文的类型，如回应请求报文，数据报超时报文等；代码域表示了该类型的几种不同情况，如当类型为 11（超时报文）时，代码为 0 表示 TTL 超时，为 1 表示片重组超时。在实现路由可达功能时要发送回应请求报文（类型为 8），过程如下：源主机向目的主机发送一个类型为 8 的回应请求报文，若目的站点收到回应请求报文则把报文 IP 头部中的目的 IP 与源 IP 地址交换，将类型 8 改为回应类型 0，计算出新的校验和再发往源主机。若源主机收到了该回应报文，则不但说明了目的主机可达，而且说明目的主机与源主机之间的路由器工作正常，源主机和目的主机的 IP、ICMP 软件运行正常。但若在传输过程中出现了某些问题，如网络不通等，导致数据被定向到一个无效的目的地，这时相关路由器或目的主机将发回目的不可达报文（类型为 3），并在代码中说明该报文的具体情况：是网络不可达还是主机不可达等。若请求报文在传输过程中超时，即 TTL 被减为 0（报文每经过一个路由器 TTL 都要减 1），则该路由器返回一个 TTL 超时报文（类型为 11），报文 IP 头中源 IP 地址即为本路由器的 IP 地址。

### 2. ICMP 追踪技术

ICMP 消息法利用了 ICMP 消息记录数据包的路径信息，使用加载了追踪机制的路由器向被攻击主机或它的上游 ISP 主动发送节点信息来为追踪提供信息来源，路由器以很小的概率（如 1/20 000）对转发数据包进行采样，并产生一个特定的“iTrace 消息”发送到与采样包相同的目的地，该消息包含采样数据包的部分内容拷贝、发送它的路由器的 IP 地址、前一跳路由器的 IP 地址、下一跳路由器的 IP 地址、时间戳以及诱发该消息的数据包的摘要和相关信息等。当遭受到攻击时，被攻击者根据收集到的 ICMP 追踪信息包（iTrace, ICMP Traceback Message）消息即可重构出攻击路径，可以构造出以被攻击端为根的攻击路径树，识别经过的路由器，如 ICMP 追踪消息、目的驱动的 ICMP 追踪、反向

ICMP 追踪。该策略类似于 PPM，不同的是它不是在 IP 包中标记，而是通过 iTrace 消息发送标记信息。其优点是与现有协议兼容，允许事后分析，无须在各 ISP 间协调，降低了管理消耗。其缺点表现在以下几个方面：

(1) ICMP 消息增加了网络负担，如果没有加密等安全机制，ICMP 消息包容易被伪造。

(2) ICMP 追踪技术使用 ICMP 数据报进行传输采样信息，与攻击数据报的类型不同，这很有可能在传输的过程中被其他网络设备，如防火墙等过滤掉，以致丢失追踪的信息。

(3) ICMP 追踪技术需要被攻击端接收 iTrace 消息才能够重构攻击路径，我们假定路由器采样概率为  $1/20\,000$ 、攻击路径长度为 20，如果被攻击端能够完整地构造出攻击路径的概率是 0.5，那么就可以计算出被攻击端需要接收攻击数据报的数量：

$$\left[1 - \left(\frac{19\,999}{20\,000}\right)^x\right]^{20} = 0.5$$

由上式可以得出以下的结果：

$$x = \frac{\ln(1 - 0.5^{\frac{1}{20}})}{\ln(\frac{19\,999}{20\,000})} \approx 67\,588$$

从上述公式中，可以看出，如果被攻击端想要 0.5 的概率来完整地构造出攻击路径，那么需要接受大约 67 588 个攻击数据报；如果把这个概率提高到 0.9 的话，则至少需要接受 104 972 个攻击数据报；如果需要尽快地构造出攻击路径，则需要提高采样概率，但是这样会给路由器增加额外的负担。

(3) 路由器在对攻击数据报采样时，受流量的影响很大，在流量小的干道，路由器采样数据很少，这直接影响到攻击路径的重构。

目的驱动的 ICMP 追踪技术在路由表和数据包转发表中引入了一个“目的位”，让被攻击者自己决定是否需路由器提供 iTrace 消息，路由器只是在被攻击者需要时发出 iTrace 消息。其优点是减少了网络流量负担，极大地改进了 iTrace 技术的性能，几乎不需要对路由选择结构做出改变，其缺点是：需要对路由设施微小的改动；由于频繁地更新路由表，会导致路由选择机制的不稳定性。

ICMP caddie 消息技术（简称 iCaddie）与 iTrace 不同的是，iCaddie 消息始终随那个导致其产生的数据包并收集沿途路由器的身份信息直至到达目的地。为防止身份信息被篡改，使用了密钥加密的哈希信息验证码。其优点是 iCaddie 消息产生的个数受攻击源的影响而不是攻击路径长度，因此能较好地应对 DDoS 攻击，但是增加了计算开销。

### 3. ICMP 定位报文法

ICMP 定位报文法的基本原理是引入新的 ICMP 定位报文。当路由器转发报文时，以极小的概率  $P$  发送对数据包的一个特殊形式的拷贝，该拷贝是一种特殊定义的 ICMP 数据包，其中加载发送它的路由器的 IP 地址以及前一跳和后一跳路由器的 IP 地址和诱发它的数据包的信息，发给目的地。当目的地收到足够多的 ICMP 定位报文时，报文传递的路径

和源头就可以确定了。ICMP 定位报文的数据区包括本地接受接口地址、上一跳接口地址、本地发送接口地址、时间戳和身份认证信息。ICMP 定位报文法的工作流程如图 8-28 所示。

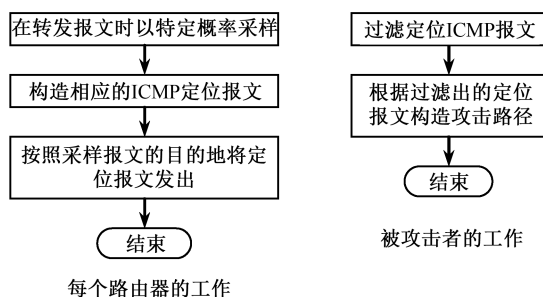


图 8-28 ICMP 定位报文法的工作流程

## 8.4.4 入口过滤法

### 1. 入口过滤的基本原理

入口过滤就是在网络的边界路由器上和网络的接入设备上设置入口过滤器和包过滤规则，对输入包的源地址进行检查，满足规则的数据包才能通过，如果发现不是合法地址，就对其进行过滤，同时进行记录。在理想情况下，数据源地址的有效值应该具有不重叠性，避免产生歧义，因此，任何进入的数据包都有唯一入口信息。即使源地址重叠，这种方法也可能是有用的，因为该方法将减少数据可能的入口点。入口过滤法的主要目的是为了防止 IP 源地址欺骗，这样的审查认证机制使网络追踪变得更加简单。

### 2. 在接入路由器上设置入口过滤

在局域网与互联网之间的接入路由器上设置入口过滤的方法如图 8-29 所示。这种设置可防范攻击从局域网进入互联网。

### 3. 局域网在三层交换机上设置入口过滤

在局域网与局域网之间的三层交换机上设置入口过滤的方法如图 8-30 所示。这种设置可防范局域网内部发起的攻击。

在默认情况下，三层交换机预防攻击的入口过滤功能是关闭的，在配置时，需要打开该服务。



图 8-29 在接入路由器上设置入口过滤

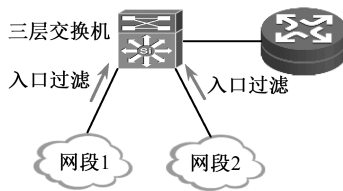


图 8-30 局域网在三层交换机上设置入口过滤

(1) 打开预防攻击入口过滤的开关：

模式：接口配置模式。

命令：Switch(config-if)#ip deny spoofing-source

这条命令用于打开指定接口的入口过滤开关。

① 这条命令只能用于三层口。

② 过滤开关打开后，系统会自动为该接口生成一个 ACL，ACL 的名称为 `auto_defeat_dos_interfaceID`，其中 `interfaceID` 是接口名。假设这个三层口的 IP 地址是 `192.168.5.1/24`，则生成的 ACL 的内容为：

```
permit 192.168.5.0 0.0.0.255
permit host 0.0.0.0
deny any
```

这个 ACL 会作用在接口的传入检查中，它只允许源地址和 `192.168.5.0` 匹配的数据报传入，以及源地址为 `0.0.0.0` 的数据报传入（这种数据报是 DHCP 请求报文），如果源地址是其他值，说明是伪造的，交换机会直接把它丢弃。

③ 你只能和在下层网段直连的接口上配置过滤功能，不要在和上层网络相连的接口（如 Uplink 口）上配置过滤功能，这会导致源自互联网的各种源 IP 报文无法进入该网段。

④ 如果在接口上有一个自定义的 ACL，则它不能和过滤生成的 ACL 同时应用。解决方法是不开启过滤功能，但在自定义的 ACL 中加入过滤用的语句。

⑤ 在设置了过滤功能后，如果修改了接口的 IP 地址，必须先关闭过滤功能然后再打开，这样才能使入口过滤对新的地址生效。

(2) 关闭入口过滤功能：

模式：接口配置模式。

命令：Switch(config-if)#no ip deny spoofing-source

(3) 查看入口过滤配置：

模式：特权模式。

命令：Switch#show access-group

本命令用于查看 ACL。

配置举例：在一个三层路由口上启用入口过滤功能。

```
Switch>enable
```

```
Switch#configure terminal
```

```
Switch(config)#interface f0/3
```

```
Switch(config-if)#no switchport
```

```
Switch(config-if)#ip address 192.168.30.1 255.255.255.0
```

```
Switch(config-if)#ip deny spoofing-source
```

```
Switch(config-if)#end
```

```
Switch#
```

配置后会生成一个名为 `auto_defeat_dos_fastethernet_3` 的 ACL，并且被关联在 `f0/3` 的传入端，它会禁止源 IP 为 `192.168.30.0` 以外的数据包从此接口进入交换机（DHCP 请求报文除外）。

#### 4. 部署网络入口过滤

部署使用网络入口过滤 IP 数据包，仅仅需要进行 IP 数据包过滤。绝大多数路由器或防火墙都支持数据包过滤功能，通过对路由器或防火墙进行配置，支持数据包过滤功能。

图 8-31 是一个典型网络入口过滤追踪框架示意图。在这个例子中，具有入口过滤功能的网络通过路由器、网关（E1、E2、E3、GW1 和 GW2）等连接到外部网络和内部网络。网络中路由器 E1、E2、E3 和网关 GW1、GW2 都已配置成具有数据包过滤功能，数据在网络中传输，通过路由器时必须是在有效的地址范围内。在图 8-31 中，攻击者通过路由器 E11 攻击被攻击主机 1，必然将暴露攻击源头存在于网络 E1 中。

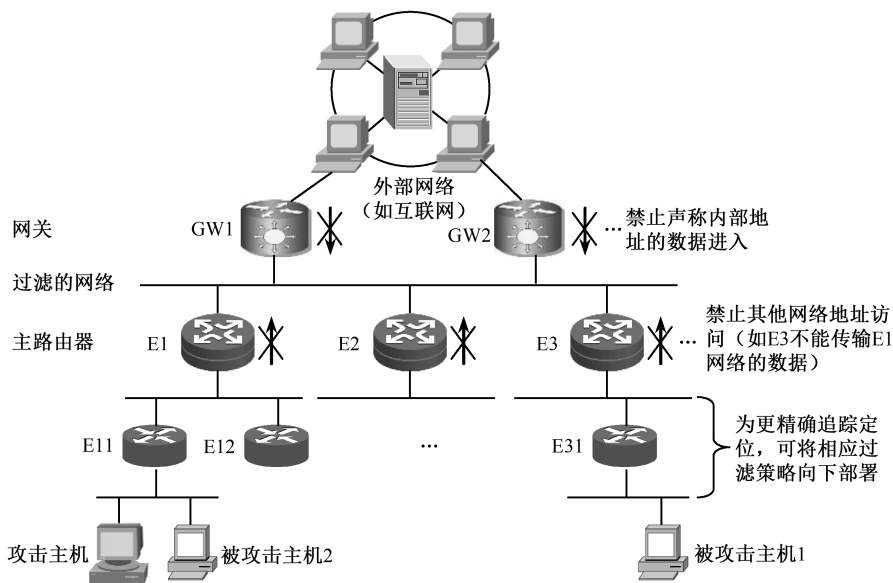


图 8-31 典型的网络入口过滤追踪框架示意图

一个典型的广域网连接到“外部”和“内部”网络，两个包过滤配置是必要的，以实现数据包过滤。

（1）连接到外部网络的路由器必须禁止传输假冒内部 IP 地址从外面进入过滤保护的网路的数据包。这是一条基本的要求，与基本的防火墙设置规则相同，可避免许多安全问题。

（2）连接到内部网络的路由器必须禁止假冒其他内部 IP 地址进入过滤保护网路的数据包。如果一个内部网络分配的 IP 地址范围 204.69.207.x（更正式为 204.69.207.0/24），路由器必须过滤（删除）没有使用来自该网段（204.69.207）的数据包。

网络入口过滤功能可以部署在更广的网络环境中，如一个更大的广域网，它下面的所有的广域网及局域网。随着越来越多的网络过滤部署应用，网络入口过滤能够提供更多、更精确的追踪信息。

基于网络过滤追踪的关键是过滤规则，需要足够精确识别到特定过滤网络的入口点。



但是将过滤规则加得太多、太细将导致庞大的路由表和复杂的管理，增大网络开销。因此，对于大多数路由器，只需要支持与其有直接联系的那一级的过滤规则就足够了。

### 5. 基于入口过滤的追踪

网络入口过滤可用于追踪，因为在大多数情况下，入口过滤迫使攻击者透露其网络位置信息。更具体地说，当受到攻击时，被攻击者能够根据入口过滤获得以下信息：

- (1) 当发生了攻击，说明网络入口过滤没有得到正确实施，工作不正常。
- (2) 网络入口过滤器（如路由器或其他网络组件）存在安全漏洞，不能有效进行过滤。攻击者利用安全漏洞绕过过滤器，实施网络攻击。
- (3) 网络攻击者的位置就在内部，甚至与被攻击者属于同一个子网，攻击数据包不需要通过过滤器。例如，图 8-31 中攻击者对被攻击主机 2 发动攻击，在这种情况下，攻击数据包需要通过具有过滤功能的路由器。在如此小的范围内进行追踪定位，将变得非常容易。

(4) 攻击数据包的源地址信息将暴露攻击者的位置信息。如果攻击从外面传来，它将有一个明确的外部地址；相反它是从内部网络传来，它将会有一个内部确定的地址或位置。部署使用多层次的网络入口过滤，消息头中的源地址将能够更加精确地确定攻击者的网络位置信息。

综上所述，基于网络入口过滤的追踪技术的优势与不足如下。

#### 1) 优势

- (1) 可以较低的成本进行部署应用，兼容性强，不少的网络路由器都支持过滤功能。
- (2) 可实现渐进部署，随着部署的增加，追踪的精度也将得到提升。
- (3) 辅助追踪，不会增加额外的存储开销（日志类）和网络带宽开销。
- (4) 对网络用户透明，不影响网络的正常使用。

#### 2) 不足

- (1) 使用网络过滤追踪技术常常只能追踪到一定范围或网络，追踪精度不够。
- (2) 不能追踪跳板等复杂的网络攻击。
- (3) 在网络路由器上实施过滤功能将影响网络路由处理性能。

#### 3) 数据流匹配追踪技术评估

网络入口过滤能追踪单包数据，能支持网络中的路由器，不能预先告知待追踪数据包的信息，追踪实施过程需要额外的通信机制，追踪精度有限。

## 8.4.5 链路测试法

链路测试法是一种逐跳追踪的方法，是反向追踪技术方法的一种，即从距离被攻击者

最近的路由器开始，交互测试其上游链路直至确定出攻击数据来自哪条链路，并按照同样的方法逐级回溯追踪攻击流经过的链路，以此达到攻击追踪的目的。在测试它的输入（上行）链路及其路由器的情况下，如果检测到了有电子欺骗的数据包（通过比较数据包的源 IP 地址和它的路由表信息），那么它就会登录到上一级路由器，并继续监控数据包。如果仍然检测到有电子欺骗的扩散攻击，就会登录到再上一级路由器上再次检测电子欺骗的数据包。重复执行这一过程，直到到达实际的攻击源。这类方法需要在攻击进行时进行追踪，如果攻击已经结束，则此类方法将失效，因而此类方法严重受制于攻击的持续时间。

链路测试主要有两种实现方法，即输入调试法和受控淹没法。

### 1. 输入调试法

输入调试法也称入口调试法。很多路由器都提供一种称为入口调试的功能，这能让管理员在一些出口端过滤特定的数据包，同时也可以检测出某一种类型的数据包到达了哪个输入端口，这种特性就被用来 IP 追踪。首先，在使用该技术进行入侵追踪时，被攻击者需确定其正遭受攻击，并且要从所有的数据包中描述出攻击报文的共同特征，然后通知网络管理员。通过这些特征，管理员将在被攻击者的上行出口处进行输入调试，在被攻击者的上游路由器处引入一条访问控制策略以检测攻击数据流来自哪个路由器。具体方法是，对所有的邻接上游路由器依次关闭它们到被攻击者或本路由器的连接（或者说过滤来自该路由器的数据包），看看攻击数据流有没有变化，如果关闭某个连接以后，攻击数据流有所减弱，则可以判断为攻击数据流经过了该连接，从而该上游路由器是攻击树的一个节点。然后在该路由器的基础上继续重复上述过程，直到追踪到攻击者或追踪过程已达其所管理网络的边界。输入调试的工作原理可以用图 8-32 表示。

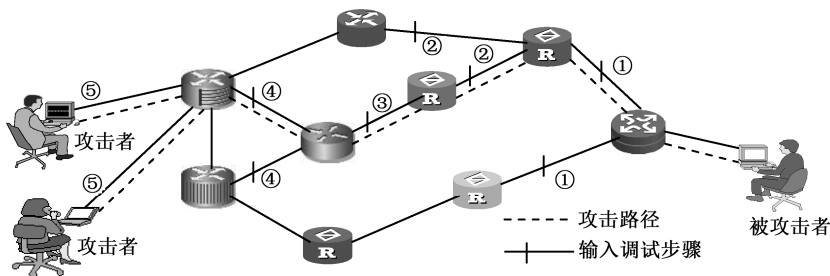


图 8-32 输入调试的工作原理

在图 8-32 中，①、②、③、④、⑤标示的是调试的步骤，对同一步中的多个连接要逐次进行测试（可以是任意顺序）。当追踪到网络边界后，该网络管理员可以通知临近网络的管理员，请求其继续未完的追踪。这种方法通常都是手工操作的，且只能到达网络边界。当跨网追踪时，不同网络的管理员之间及时的通信和合作是必不可少的，而在实际中，这种办法最大的问题就是管理花费，要联系多个 ISP，而且同他们合作需要时间，因此这种办法需要大量的时间，而且几乎不可能完成。

这种方法与现有的协议、现有路由器和网络基础结构兼容，支持新增的实现，几乎不

需要再添加网络软硬件设施。该技术是攻击源反向追踪的基本技术，只有在攻击进行的过程中有效，不适于事后检测。而且，该技术带来的管理负担比较重，操作复杂，追踪速度慢，如果没有合适的网管人员，或者网管人员缺乏技术支持，输入流量调试将无法进行。

## 2. 受控淹没法

受控淹没法的基本思想是通过猝发的大量报文去淹没与其直接相连的链路，通过观察对攻击者的影响来定位攻击源。被攻击主机首先需要掌握整个网络的拓扑情况。然后，对可能位于攻击路径上的路由器发送突发性的流量，观察对攻击流的影响。被攻击主机使用已知的拓扑结构图，选择最接近自己路由器的上游链路中的主机，对这个路由器的每个输入网络链路分别进行强行淹没。由于这些数据包同攻击者发起的数据包同时共享了路由器，因此增大了路由器丢包的可能性；若此攻击流量位于攻击路径，则发送突发性流量必然导致路由器丢包率增加，使攻击流减弱。被攻击者通过观察各连接的数据包变化率，可以推断出攻击流量来自哪个连接；同其他的连接测试一样，与它的上游路由器重复这过程直至攻击源点。受控淹没的工作原理可以用图 8-33 表示。

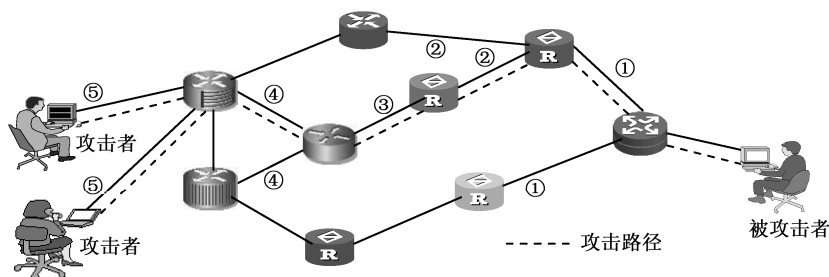


图 8-33 受控淹没的工作原理

在图 8-33 中，①、②、③、④、⑤标示的是调试的步骤，对同一步中的多个连接要分别发送“洪水”进行测试，若其中对某一个连接发送“洪水”后使得攻击报文减少，则认为这条连接参加了攻击报文的发送。与输入调试法相似，当追踪到网络边界后，该网络管理员可以通知临近网络的管理员，请求其继续未完的追踪。由于这种方法也基本由手工操作组成，因而这种办法需要大量的时间，并且对其他未遭受攻击的连接影响太大，因此很难完成。

受控淹没法与现有协议、路由器和网络基础结构兼容，不需要修改路由器的设置且对路由器的开销很小。但该方法的缺点是：首先，它不具有事后处理能力，只有在攻击行为正在进行时才能成功；其次，该方法本身就是一种拒绝服务攻击，这可能会破坏信任的上游路由器和网络上的有效业务；再次，该方法对于相对复杂的网络拓扑结构实现起来比较困难，需要被攻击者有一张很好的覆盖大部分互联网拓扑图和一张淹没主机的联系表；最后，该方法对 DDoS 攻击难以奏效。连接测试机制本身就比较繁杂，当某一路由器在攻击时有着多个上游连接时，它很难通过区分不同路径来进行路径搜索。

#### 8.4.6 层叠网络追踪

典型路由器的配置是为了更快地转发数据报，而不是用来分析或追踪报文。一台路由器所具有的最基本追踪功能是可以提供某 IP 包进入该路由器的输入端口，然后据此可以找到该 IP 包经过的上游路由器（主干网高速链路上的路由器不提供这些基本功能）。

层叠网络追踪的基本思想是：首先，利用 IP 隧道技术把边界路由器和一些用于追踪的路由器直接连接起来，建立一个层叠的逻辑网络，对于所有可疑的流量，从边界路由器到追踪路由器都会被重新路由；当检测到攻击时，让攻击包通过该逻辑网络传输，这样可以通过边界路由器对流量进行监视；逻辑追踪网络根据攻击数据包进入该网络的入口判断其上游链路的边界路由器，追踪网络上的数据包会再一次经过检查，然后根据检查结果决定丢弃该包或将其转发到相应的出口。

下面以图 8-34 为例来说明层叠网络的追踪问题。主要引入了网络中的追踪路由器（R7 或 R8）。该路由器监管所有流经网络的流量，为了实现这一目的，所有数据包必须经由该路由器形成路由。这可通过为每个边界路由器（R1—R4、R6、R9、R11 和 R12）到追踪路由器创建一个公有路由封装隧道来完成。一旦边界路由器和追踪路由器上配置了适当路由，所有进入边界路由器的网络流量将会流经由路由封装隧道到达追踪路由器，再从追踪路由器经过另一路由封装隧道到达出口边界路由器。当核心路由器输送流量时，从逻辑上讲它只是从一台边界路由器直接到追踪路由器的一跳而已。这种结构可被视作以追踪路由器为中心的网络中，所有边界路由器通过路由封装隧道与追踪路由器相连的星型拓扑结构。隧道建立在已有拓扑结构上，利用已有路由协议，这个类似星型的逻辑网络被称为层叠网络。当然，实际上单个追踪路由器不能处理来自整个网络数据包负载。因此，这是一个在物理上全互联、在逻辑上仍被看作单一追踪路由器的几台追踪路由器相连的网络。这与所有其他方法不同，入侵检测是被攻击者的功能。当一次攻击被检测到时，意味着有一个单一数据包或组成侵扰动作的数据包序列，因为只有一跳距离，攻击的源头可以被识别。另外，ISP 必须在确定攻击同时完全靠自己执行一次追踪，他们也将不得不大量购买追踪路由器和 IDS 服务器，因此该方法涉及的 ISP 很多。通过给网络增加边界路由器导致配置追踪路由器以便于能实现追踪。该方法的局限性是：它将仅在一个单一主权领域有效。为了使之在跨诸多 ISP 的层叠网络中的功能也很好，有必要设法将所有追踪路由器连接成一个系统。

虽然层叠网络追踪方案不仅简化了逐级追踪，并且能追踪，而且还能通过丢弃攻击性数据包而起到防范攻击或至少减轻攻击力度的作用，只需要利用现有的协议就可以很快地找到攻击包的入口点。但也存在严重问题，具体表现在以下几个方面。

（1）它对网络拓扑先验知识的依赖性大，构建层叠网的操作复杂。

（2）建立和维护 IP 隧道会给路由器造成不小的额外开销，如果攻击者对主干高速路由器进行拒绝服务攻击，这种处理可能导致放大攻击的负面效果。

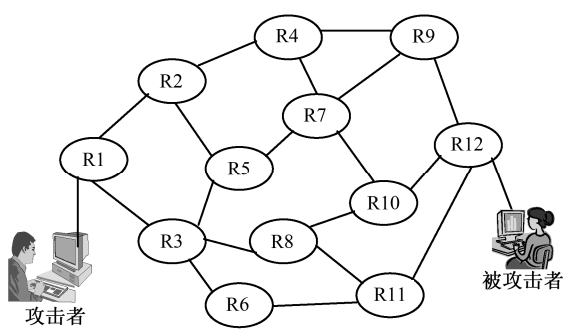


图 8-34 层叠网络追踪的网络拓扑示意图

- （3）如果与追踪网络相连的边界路由器被攻击者控制，那么边界路由器不会将数据包路由到追踪网络，需要边界路由器根据数据包特征动态调整路由。
- （4）由于近年来路由器受到攻击的事件不断增加，要保证所有边界路由器的安全在实际中是非常困难的。
- （5）使用 IP 隧道需要对数据包进行额外封装，在大流量攻击时，这些额外封装有可能导致 IP 隧道崩塌。
- （6）该方案依然是将所有可疑的攻击性数据包都转发到追踪网络中，没有改善层叠网追踪的性能，反而会增加网络的额外负载。
- （7）仍然需要进行接入调试，并依赖管理员的人工处理，需要 ISP 之间的协作，而且攻击者容易使用一些工具如 Traceroute 发现路由策略的变化而改变攻击的策略。

8.4.7 IP 源追踪技术的比较

每一种 IP 源追踪技术都有其自身的优点与缺点，目前还没有一种技术在各个方面都有绝对的优势，可以通过表 8-1 对上面讨论的 IP 源追踪技术进行比较。

表 8-1 IP 源追踪技术比较

参数追踪技术	追踪速度	管理负担	网络负载	路由器负载	对 DDoS 的追踪能力	事后追踪能力	与 TCP/IP 的兼容性	与路由器的兼容性
PPM（概率性数据包标记）	较快	较低	较低	较低	一般	较好	差	差
路由记录	较慢	较低	低	较高	较好	好	好	好
ICMP 消息	一般	较高	较低	较低	较差	一般	较差	较差
入口过滤	较慢	高	高	高	较好	无	好	好
输入调试	较慢	高	低	低	差	无	好	好
受控淹没	较慢	高	高	高	差	无	好	好
层叠网络	较慢	多	高	高	较好	无	较好	较好

通过表 8-1 的比较可以看出, PPM (概率性数据包标记) 要对 IP 数据报的格式重新定义, 因此与 TCP/IP 的兼容性大大降低。路由记录其他各个方面都较为突出, 但是由于需要路由器存储用于追踪的日志信息, 因此对路由器负载要求较高。ICMP 消息需要定义新的 ICMP 报文类型, 另外需要特殊功能的路由器, 不管是与 TCP/IP 的兼容性还是与路由器的兼容性都较差。入口过滤技术由于需要路由器判断每一个 IP 地址是否是合法源地址, 因此路由器负载重, 另外对 IP 地址的管理也需要网络管理人员人工操作, 无法实现自动化, 因此不适合目前网络流量背景下的追踪。输入调试、受控淹没难以实现自动化过程, 对网络管理人员负担太重, 也不太适合目前的网络追踪。层叠网络对 DDoS 的追踪能力、协议与路由器的兼容性都较好, 但是会增加网络的额外负载, 构建层叠网的操作复杂。

虽然没有一种技术占有绝对的优势, 但是通过分析, 我们可以看出, 路由记录技术与目前的 TCP/IP 体系完全兼容, 比较容易实现自动化, 并且事后追踪能力最为突出, 如果要较好地解决路由器负载问题, 应该是一种成本较低, 效率较高的追踪技术。

#### 8.4.8 IP 源追踪面临的关键问题与研究展望

上述的各种追踪技术可以说各具特点, 但又都存在一定的缺陷。综合起来, 可以看出一个理想的追踪方法应该是在性能和负荷, 网络负荷和受害终端负荷以及硬件与软件之间做出一种合理的选择分配; 在被攻击者受到大规模攻击时, 以尽可能少的资源消耗、更快的收敛速度、更小的计算负担、更高效的处理能力、更低的误报率、更准确的判断能力追踪到攻击的始作俑者, 并重构攻击路径。

##### 1. 面临的关键性问题

对于现有的网络状况, IP 源追踪技术依然面临以下关键问题。

(1) 互联网对于报文的接收者缺乏有效的认证机制, 从而无法判定该报文是否真实地来自报文中的源地址。虽然给每个设备均分配一个地址, 但仍无法阻挡攻击者伪造地址。由于数据包的源地址是由发送方自行填入, 因此攻击者可以伪造或通过代理改变其源地址信息, 从而隐藏真实源地址。

(2) 攻击者通过控制足够多的傀儡机, 使得攻击流被充分“稀释”, 其大小接近合法流, 这种攻击流的“稀释效应”大大增加了检测和预防攻击的难度。

(3) 当前的网络攻击出现大范围、跨国界的状况, 防火墙的使用使得现实中 IP 追踪只能识别到局域网的入口点; 或者攻击源的“跳板”, 很难通过防火墙进入局域网内部。

(4) 高速网的建设及高速设备的投入使用阻碍了现有的跟踪算法的应用范围。

虽然人们已提出了许多解决方案, 但目前的研究成果与实际网络应用之间尚有较大差距, 大部分已提出的 IP 追踪技术依然处于试验应用阶段, 至今还无法在互联网上广泛使用。在当今网络协同工作的大环境下, 信息的保护和网络设施的安全防御尤为

重要, IP 追踪所要面临的情况也越来越复杂, 因此对网络攻击源的追踪技术需要更加深入的研究。

## 2. 研究展望

下面从以下几方面归纳 IP 源追踪需要进一步关注的问题及其研究方向:

(1) 随着 IPv6 技术的推广、高速网和无线网络的建设, 如何将现有的追踪方法进行移植, 利用中转点进行追踪和信息识别, 以及根据新问题的特点提出更高效更可靠的追踪方法将是 IP 源追踪研究中需要关注的问题。

(2) 在实名认证机制不健全的网络环境下, 如何结合安全管理(如通过实名认证、IP 与 MAC 地址绑定等方法)消除源地址的匿名性也值得研究。

(3) 对于不同层次的网段, 如何协调追踪规则, 制定不同的追踪策略, 需要一些规则来处理追踪结果, 在不侵犯隐私的前提下更高效地识别攻击源信息也是需要关注的问题。

(4) 如何将 IP 追踪技术与数学编码思想结合, 有效地减少重构路径所需的数据包数量, 降低漏报率和误报率, 提高追踪效率。

(5) 如何将 IP 追踪方案直接用于 IPv6, 或在 IPv4 与 IPv6 的混合网络中有效实行, 也是下一步的研究重点。

(6) 各种 IP 源路由追踪算法都需要迫切解决的问题是算法的实际可运行性。如何找到一种简单的、实施方便、极易标准化的方法来解决 IP 协议中的源地址问题仍将是研究人员的探寻方向。

(7) 构建网络追踪系统的硬件平台, 建成一整套的网络追踪解决方案, 组建成由软、硬件结合的网络追踪系统。未来, IDS 和 IP 追踪系统的联动将是焦点问题。

(8) 如何解决追踪系统的配置问题。大多数追踪技术要求对网络进行一定的改变, 包括增加路由器功能和改变分组。为了推广追踪技术应用, 应在实现时减少这些要求, 尽量做到与现有网络兼容。

(9) 在提高 IP 追踪技术的功能时, 如何保证其安全性也值得关注。为保护隐私还应有一些方针来指导处理追踪结果。

(10) 追踪精度和追踪开销的矛盾始终存在, 如何在其间选择一个平衡点是需要权衡的问题。可以考虑在新协议中支持控制资源消耗, 从而使攻击比追踪需要更多的资源消耗。

(11) 建立量化的评估指标体系, 评估 IDS 和 IP 追踪系统得到结果的正确性, 系统地比较当前各种方法的优劣, 进一步完善现有算法。

(12) 建立网络攻击源追踪的理论模型。由于追踪在复杂的互联网上进行常常是耗时和低效的。因此需要建立包括攻击模型、追踪模型、追踪环境模型等的一整套网络攻击源追踪的数学模型, 以便更全面系统地解决攻击源追踪任务。

(13) 考虑多播、移动性、主动协调性、IPv6、数据加密等问题。如何改进已有方法使之适合新的问题, 或根据新问题的特点提出更简单可靠的、新的追踪方法值得仔细研究。

## 8.5 面向连接链的追踪技术

网络攻击者通过使用各种匿名技术隐藏真实身份，在到达被攻击者之前，一个连接的攻击流经过一系列的中间主机（跳板机，阶石主机）构成的链称为连接链。图 8-35 为一个连接链的简化示意图，其中， $-m, -m+1, \dots, n$  表示阶石主机。攻击者从  $-m$  登录到  $-m+1, \dots, n-2$ ，最后在  $n-1$  发起对  $n$  的攻击。



图 8-35 连接链的简化示意图

连接链攻击容易实现和使用，然而，发现攻击者的真实身份却非常困难和复杂。连接链追踪确定真正攻击主机的关键是中间节点的输入和输出连接的关联（流匹配）。由于使用加密、压缩引起内容改变或系统延迟引起时间改变，流匹配操作更加复杂，并且网络入侵在高速网络上进行，要求中间节点关联必须是实时的。如果不能有效而快速发现攻击源，就不能制止有可能继续发生的攻击并惩治攻击者。

针对上述问题，下面介绍三种面向连接链的追踪技术，即基于网络的连接链追踪、基于主机的连接链追踪和基于主动网络的连接链追踪。

### 8.5.1 基于网络的连接链追踪技术

该技术借鉴了“连接链”概念，一些嗅包器被安排在网络合适点上，每一个点都收集 TCP 流的信息。这些流按一定的时间间隔被分隔，通常是一分钟长度。用 128 个向量来指向 128 个 ASCII 码在流中出现的次数，形成“指纹”。利用嗅包器收集的信息，通过分析跳板主机之间 TCP 连接的属性和特征，采用信息摘录技术，把攻击报文流同其他报文流区别开来，从而发现攻击报文在网络中的穿行路线。为了尽可能地收集连接信息，需要在网络中设置大量的嗅包器。当检测到有入侵发生时，就会通知所有的代理立即对监听的每个连接进行摘录比对，凡是符合入侵报文特征的连接就是入侵路径中的一段，如此可以一直追溯到入侵源或系统覆盖的边缘。这种技术可以追踪分布式的网络入侵，系统负担小，由于是实时激发的，在没有入侵的情况下几乎不占用任何网络带宽和系统资源。但缺陷也是显而易见的，它只能追踪正在发生的网络入侵，一旦入侵行为结束，入侵报文在信道中销声匿迹，就无法进行信息摘录了，即没有任何事后追踪的能力。该技术也不能对加密的信息进行信息摘录，并且需要系统时间同步。



该技术通常用于追踪采取远程登录进行攻击的黑客，在一连串连接链中，每条信道都负载着多个网络连接，而传送相同报文的连接特征必定是相同的，因此就可以找出某个攻击报文通过的信道路径。但是如果对连接中的所有信息都进行比对，则会浪费大量的存储空间，带来过多的处理负担，这就需要对连接内容进行摘录和归纳。

基于网络的连接链追踪技术是根据网络连接的属性来进行追踪的。具体实现方法有指纹技术、网络纹印技术、基于时间的连接链追踪技术、基于偏差的分析技术、连接内容分析、TCP 序号分析和入侵识别与分辨协议。

### 1. 指纹技术

指纹是一种最早的关联技术，它利用了少量的信息去概括连接链的信息，对连接内容进行摘录和归纳。理论上它能够从许多不相关和相关的连接链中唯一识别出处于相同路径中的一条连接链。指纹技术具有数据量少、内容敏感度高、鲁棒性、可追加性、易于计算、易于比较的特性。其缺点是依赖严格的时钟同步，不适于实时追踪。

### 2. 网络纹印技术

网络纹印是一种先进的网络技术，通过对网络传输协议的研究发现，可以通过一组数据描述网络的连接特征，该数据随着网络的不同连接而不同，网络纹印可以理解为网络标志，对于不相关的网络连接，网络标志完全不同，对于相关联的连接则有相似之处。因此通过记录网络入侵状态下不同节点的网络标志，整个网络范围内对同一时刻不同网络节点处的网络纹印比较，发现网络入侵的攻击轨迹。网络纹印的优点是空间占用量非常小，但是需要在网络所有的网段中安装专门的软件收集网络纹印数据，而且网络纹印数据只能被网络跟踪专用，不能用来分析网络的数据流量或入侵检测使用。在网络环境中的时钟同步以及数据传输过程中的延迟问题也影响网络纹印的准确性。采用该种方式在传输网络纹印数据时也容易被攻击，这限制了该方式在实时跟踪方面的应用。

### 3. 基于时间的连接链追踪技术

基于时间的连接链追踪技术是用于解决连接链中跨越多重跳板的一种追踪技术。该技术收集网络中每个检测点的有关数据，包括网络传输数据包的大小以及传输时间等内容，不包括网络数据包的内容。一般而言，如果两个网络连接处于同一个连接链中，则当攻击者沿着连接链传送数据时，数据流在链路各个连接中具有相同的时间特性。也就是说，在某个时刻，连接链中不同的连接同时有数据传输，而在其他时刻，又同时处于空闲状态。当然，网络会在不同连接之间引入一定的时延。因此，可以在网关中部署网络嗅探器，记录所有网络连接数据传送的开始和结束时间，据此来分析连接链。

开始时间是一个网络连接中开始数据传送的时间，结束时间是数据传送结束的时间。通过分析网络连接的数据传送开始和结束时间，并把二者相关联，就有可能找到攻击者的踪迹。如果两个连接  $C_i$  和  $C_j$  传送数据的开始时间相隔较大（大于给定的值），或者在某些场合  $C_i$  的开始时间早于  $C_j$ ，而在其他时候， $C_j$  的开始时间却又比  $C_i$  早，那么，这两个连

接肯定不处于同一个连接链中。

通过对这些信息的分析，将相关的网络数据链连接起来，构成网络入侵行为的全过程。这种方法只是利用了分组的时间，相对于前面提到的方法而言，适应性较强，它可以用在加密的环境中。虽然该技术不需要网络时钟同步，防止数据转发中的变异，但它也存在一定的局限，该方法的计时特征包括了建立连接的整个过程，如果攻击者在进入和外出连接之间人为地加入一些时延，则可能导致时间分析方法的失败，很难应用到实时跟踪当中。

#### 4. 基于偏差的分析技术

基于偏差的分析技术定义了 TCP 协议传输时数据包之间的最少平均延迟时间为偏离，使用两个 TCP 连接序列号的最小平均差别来确定两个连接是否关联。它在网络中的主机受到入侵时，该主机有可能被用作攻击其他主机的跳板，计算该主机数据包的偏离值并与网络中所有主机的偏离值相比较，如果某个主机的偏离值相近，说明这两个主机是在同一连接链上，反映了入侵行为在网络中的行为轨迹。该方式不需要时钟同步，而且防止数据转发过程中的变异，但是由于计算偏离需要记录连接过程中的所有数据包，很难应用到实时跟踪，另外还有一个缺点就是该方式只能应用到 TCP 网络中，只适合于检测交互式“跳板”，并且无法直接用于加密或压缩的连接。

#### 5. 连接内容分析

这种方法的主要目的是在不修改任何网络协议的前提下，确定一个连接链，对网络攻击进行事后追踪分析。主要思想是在网关中放置嗅探器（Sniffer），监视所有活动的网络连接，从活动连接的 TCP 数据段负载中提取连接特征。特征提取主要是统计连接传送的数据中字符出现的频率，并把计算结果作为当前连接的特征。如果检测到网络攻击，则把嗅探器收集到的数据汇总，进行统计分析，提取连接特征，找出具有相同特征的连接。这种方法对基于文本的网络协议（如 Telnet、Rlogin 等）有较好的效果，但是却无法处理采用加密或压缩技术的网络连接。此外，私自检查网络数据流在某些地区可能是非法的。

#### 6. TCP 序号分析

这种方法通过分析 TCP 数据段的序号和时间来追踪入侵者，而不依赖于数据段中的内容，因而可以用在某些加密环境中。

在这种方法中，首先在网关中记录每一个连接中 TCP 数据段的序号，并以时间为  $X$  轴，序号为  $Y$  轴作曲线。如果两个连接  $C_i$ 、 $C_j$  处于同一个连接链中，那么  $C_i$  和  $C_j$  中 TCP 数据段的序号增长速率相同，绘出来的曲线几乎相同。唯一不同的只是因为网络时延和初始序号的不同而带来的  $X$  轴和  $Y$  轴的平移。

如果网络采用链路层加密，这种方法则无法正常工作，因为 TCP 数据段的头部已经被加密。如果在连接中采用了不同的压缩技术，此方法也会遇到阻碍，在这种情况下，采用数据压缩技术的连接中 TCP 数据段序号增长速率较慢。

## 7. 入侵识别与分辨协议

入侵识别与分辨协议采用主动方式跟踪入侵的路径,并定位入侵者的位置。它的工作方式是通过入侵检测系统收集交换检测到的信息、入侵名称、攻击方式描述等,但是不需要记录所有的相关连接信息。入侵识别与分辨协议需要在防范系统的主机上安装相同的入侵检测系统。它的跟踪效率与防范范围内的入侵检测系统的检测效率,以及对入侵方式描述有关,这些因素直接影响了跟踪的效率。

## 8.5.2 基于主机的连接链追踪技术

基于主机的入侵追踪就是以被保护的主机为追踪基础,驻留在主机中,通过审计和监视经过主机的网络报文,以及与其他主机交互,来完成入侵追踪功能。

攻击者一般不会通过他自己的主机来发送伪造的 IP 数据报。源主机  $H_0$  在对目标主机发起攻击前,一般先要寻找一些有漏洞的主机,然后以这些主机为跳板,取得对它们的控制并使之成为协助自己进行攻击活动的工具,从而方便进行远程控制和隐藏自己的真实位置;经过多次登录后,在登录链  $H_0, H_1, \dots, H_n$  的最后一个主机  $H_n$  (傀儡攻击主机)发起攻击。所以,要确定攻击者的源主机,还必须对源主机到攻击主机的连接链进行追踪。下面介绍几种典型的基于主机的连接链追踪技术与方法。

### 1. 因特网环境身份识别系统 (CISIE, Caller Identification System in the Internet Environment)

#### 1) CISIE 简介

基于主机的连接链追踪技术的一个典型代表就是 CISIE。它工作在封闭的集中主机控制的网络环境中,由管理员进行统一控制和管理,所有的报文必须由管理员控制的机器产生。CISIE 是为了在多台跳板主机追踪入侵者而设计,它的目标是向处于扩展连接的主机报警,提供前若干跳的连接信息。这样,被保护主机就可以据此来做出是否允许登录请求的决定。

CISIE 系统由两部分组成:身份识别服务器 (CIS, Caller Identification Server) 和扩展的 TCP 封装 (ETCPW, Extensional TCP Wrapper)。CIS 负责跟踪每个远程登录到主机的用户;ETCPW 负责当有用户请求登录服务时,通知本地的 CIS 进行追踪。

CISIE 的工作原理和过程:主机接收到有用户请求登录服务的信息时,ETCPW 指示本地的 CIS 形成对该登录进行追踪的请求,发送给前一跳主机的 CIS。该请求包括用来识别 TCP 连接的 TCP 端口号和主机地址。前一跳主机的 CIS 收到请求后,返回拥有该 TCP 连接的用户号,本地 CIS 存储该信息以备后用。然后,从被保护主机的 CIS 开始,依次向它的前一跳主机的 CIS 核对用户身份的真实性,即本地存储的用户号信息和前一跳主机中的是否一致。如果均一致,则允许该用户登录;否则,拒绝登录请求并报警,说明有假源

地址欺骗的情况发生。

## 2) CISIE 系统的实现

在 CISIE 系统中,ETCPW 部分使用的是由 Wietse Venema 开发的著名的 TCP 封装的扩展,它对 TCP 封装的功能做了一些修改,使之不仅能够向应用程序提供 TCP 连接两端的 IP 地址,还能提供端口号。当被保护主机接收到远程登录请求时,TCP 封装就启动一个线程,把包含在登录请求中的 IP 地址和端口号传递给本地的 CIS,接着 CIS 据此来发送追踪请求。当追踪过程结束,CIS 将结果传递给 ETCPW,由 ETCPW 把结果标准化输出并调用脚本程序来允许或拒绝本次连接请求。

为了防止恶意的攻击者冒充前一跳的 CIS,或者请求 CIS 追踪合法的用户以达到扰乱系统工作的目的,CISIE 系统采用了一些安全措施来确保会话的安全。由于绝大多数的 CISIE 交互都是客户机请求和服务器的响应,因此可以使用服务器的公钥来加密客户机端的请求,并在请求信息中加入随机数。服务器可以在响应信息中返回此随机数,并用客户机的公钥进行加密,使用自己的私钥对响应信息签名。由此避免大多数形式的回放攻击。

## 3) CISIE 系统的评价

CISIE 系统可以追踪到出现地址欺骗情况的主机,从而保护系统免受可疑用户登录造成的影响。但也存在着缺陷:第一,CISIE 系统只能工作在封闭的集中主机控制的环境中,在开放的环境下不能有效地进行追踪;第二,CISIE 只能用于实时的追踪,即在攻击动作结束之前进行追踪,而一旦攻击停止,所有连接信息都将消失,追踪就无法进行下去。

## 2. 分布式入侵检测系统 (DIDS, Distributed IDS)

DIDS 的主要思想是:在 DIDS 域内的每一台监控主机收集网络中活动用户的有关信息,对这些信息进行审计,并将审计结果发送到一个中央处理服务器中进行综合分析;DIDS 记录网络中所有用户的活动状况,通过记录网络系统中的所有用户的活动信息实现该网络内的跟踪。缺点是由于保存域中所有用户的登录信息并进行集中分析,无法用于处理互联网中巨大的信息量;DIDS 通过集中控制的方式监控整个网络的活动,这对于互联网或大型的网络则不适用,因此,DIDS 只能运行在小型的局域网中。

## 3. Caller ID

Caller ID 是美国空军采用的一种网络跟踪方法。但是 Caller ID 却是备受争议的,因为它采用了与网络入侵者相同的入侵手段,沿着与网络入侵相反的路径进入网络中的其他系统,直至追踪到入侵者所在的位置。Caller ID 与其他两个系统相比,它可以运行在互联网上,对网络的规模没有限制,而且效率较高,不需要花费太多的系统资源。Caller ID 与网络入侵同步进行,即网络入侵者在进行入侵行为的同时,Caller ID 采用相同的方式反跟踪入侵者的原始位置,但是当攻击者攻击速度快、时间短,很快结束攻击行为,或者网络入侵者将入侵时采用的一些安全漏洞关闭,用 Caller ID 进行跟踪会很困难。而且手动追踪速度较慢且容易被攻击者发现,还受到一定的法律约束,跟踪的隐蔽性也不好。

基于主机的跟踪系统的基础是主机的信任问题,该系统将监视系统设置在信任的主

机上,同时这些信任主机之间的数据通信也非常关键。如果其中一台主机被攻击,该主机提供的通信数据可能是伪造或被修改的,那么该跟踪系统就无法准确地跟踪到入侵者的位置了。

### 8.5.3 基于主动网络的连接链追踪技术

基于主动网络的连接链追踪技术和基于一般网络的追踪技术的不同在于:它通过分布在网络各处、合适位置的代理,把网络连接成一个整体,不仅能够进行入侵检测和追踪,还可以加入响应功能,对入侵行为进行拦截和反击。这些代理互相之间通过协助和通信来完成追踪和响应动作。基于主动网络的连接链追踪技术有以下三种:

#### 1. 网络入侵源点的安全管理识别 (DecIDUouS, Decentralized Source Identification for Network-Based Intrusions) 系统

在 DecIDUouS 中有两个核心概念,第一个是动态安全连接的概念,它建立在 IP 安全协议 (IPSec, IP security protocol) /因特网安全关联和密钥管理协议 (ISAKMP, Internet Security Association and Key Management Protocol) 结构之上。IPSec 的核心概念就是在两个网络实体之间的安全连接关系 (SA, Security Associations), SA 的基本服务选项包括认证和加密;而 ISAKMP 是为 SA 的建立、选项协商和拆链服务的。DecIDUouS 系统是通过攻击报文所经过安全连接的位置情况来推断出攻击源信息的。第二个核心概念是在不同协议层上的 IDS 和攻击源识别系统的管理信息集成,它预留了向低层协议的接口,使得无论是应用层还是网络层的 IDS 都能与之良好合作。

**DecIDUouS 系统的工作原理:** DecIDUouS 系统利用了 IPSec 对报文来源的认证功能作为入侵追踪的基础,由于 IPSec 报文头中的地址不可能假冒,因此 DecIDUouS 就可以根据这些真实的地址追溯到报文的源头,而不受假源地址的干扰。

一个用于确保 IP 地址可信的方法就是在任意两个需要通信的网络实体之间建立 SA,但这个代价过于昂贵和死板。这就导出了“动态安全连接”的概念,即动态地决定在何处、何时建立 SA,并撤销无用的 SA。DecIDUouS 系统的运行还有一个假设,即所有的路由器都遵循“最短路径转发”原则,并丢弃那些不符合该原则转发来的报文。

图 8-36 描述了一个有 6 个节点的线性网络拓扑情况,假设这 6 个节点在同一个管理域内,可以任意建立安全连接。其中节点 F 为攻击目标。当节点 F 遭受不明来源的攻击时,运行在 F 上的 IDS 系统将检测到有攻击发生,并将情况报送 DecIDUouS 系统。接着 DecIDUouS 系统按照某种算法 (通常是选择中间点) 来确定第一个安全连接的建立位置,在图 8-36 中认证头标 (AH, Authentication Header) 为 C 和 F 节点,选择了节点 C,这就意味着节点 C 将负责转发和认证所有目标为节点 F 的报文。如果在 IDS 继续检测到的攻击报文中,有的报文经过节点 C 的认证,而另一些没有,就可以判定至少有一个攻击源在

节点 A 到 C 之间，其他的攻击源在 C 到 F 之间。这样以节点 C 为分界，将线性拓扑分为两个攻击带。接下来在这两个攻击带之中分别建立安全连接，逐步缩小范围。例如，在节点 A 建立安全连接，如图 8-37 所示。



图 8-36 线性网络拓扑攻击图一

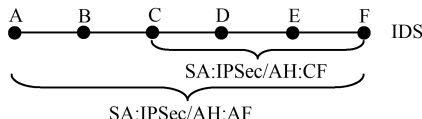


图 8-37 线性网络拓扑攻击图二

如果在后续收到的攻击报文中没有经过节点 A 认证，则可推断攻击源来自节点 B、C 或它们中间的连接。对于一般网络拓扑，DecIDUouS 系统将把它映射为线性拓扑，然后分别按照以上两种情况处理。在此引入了最短路径的概念：所谓节点  $V_x$  和  $V_y$  之间的最短路径  $(V_x, V_y)$ ，就是在  $V_x$  和  $V_y$  之间最少的跳数。映射算法从攻击目标出发，将网络中的节点按照与攻击目标最短路径递增的顺序排列，从而把一般拓扑转换为线性的排列。

DecIDUouS 系统在接收 IDS 报送的报文信息同时，它会判断对攻击的检测是否已经包括在已经建立的攻击区中。若不是，就需要建立一个新的攻击区来追踪攻击。另外，DecIDUouS 还需要判断一个新的 SA 是否需要建立、老的 SA 是否需要拆除，并负责更新本地的安全政策库。

DecIDUouS 系统的局限性在于它只能追踪正在发生的攻击，它需要在攻击的进行过程中，通过不断建立安全连接来确定攻击源的位置。一旦攻击结束，无法搜集更多的信息，DecIDUouS 系统就失效了。

## 2. 协同入侵追踪和响应框架 (CITRA, Cooperative Intrusion Traceback and Response Architecture)

CITRA 使得入侵检测系统、路由器、防火墙、安全管理系统和其他系统能够相互协同起来，实现以下四个目标：①在网络边界内追踪入侵者；②阻止或减少入侵造成的后续破坏；③汇报入侵活动情况；④在网络范围内进行协同的入侵响应。换言之，CITRA 是一个集中式的体系结构，它把独立开发的组件进行低成本的集成，并使得对其中的任何组件可进行灵活修改。

CITRA 能够同时完成入侵追踪和响应这两大功能，它的核心部分引入了一个新的协议，称为入侵检测和隔离协议 (IDIP, Intruder Detection and Isolation Protocol)，这是一个应用层的协议，用来协调入侵追踪和隔离。使用 IDIP 协议的系统被组织为若干 IDIP 社区，以此为进行追踪和协同的基本单位。每个 IDIP 社区就是一个管理域，其中负责入侵检测和响应功能的系统被称为发现协调器 (DC, Discovery Coordinator)，它是 IDIP 社区的核心。一个 IDIP 社区内可分为若干邻居域，邻居域是使用 CITRA 体系的系统集合。邻居之间通过边界控制器 (BC, Boundary Controller) 互相连接起来。

IDIP 的设计目标是实现各系统之间的信息共享, 以达到进行协同追踪和响应的层次。IDIP 社区中的每个系统都必须负责存储报文信息或网络连接情况, 一旦有攻击发生, 即可相互进行信息交换和查询。系统之间的相互协作主要通过互发消息来完成。

IDIP 协议是一个双层的结构, 分为应用层和消息层。应用层完成入侵追踪和隔离, 使用三种消息类型: 追踪消息、汇报消息和 DC 指令。消息层的功能是为应用层通信提供安全保障, 对消息进行加密、认证, 起着安全传输平台的作用。

图 8-38 描述了一个 IDIP 社区, 由三个邻居域组成, DC 在第一个邻居域中, 邻居域之间用边界控制器 BC 相连。

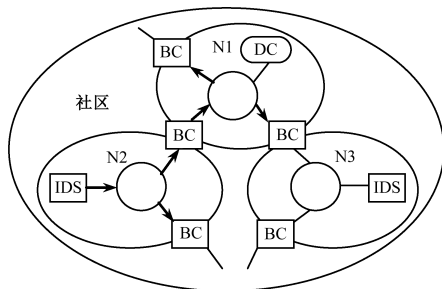


图 8-38 IDIP 社区

图中的箭头描述了当有攻击发生时, IDIP 社区是如何进行追踪的: 第一步, 入侵检测系统检测到有攻击发生。第二步, 入侵检测系统随即向它的每一个邻居节点发送追踪消息。该消息包括了对攻击事件的描述和/或对入侵连接的描述。这样其他的 IDIP 节点就可以根据这样的信息来判断自己是否处于攻击路径上。第三步, 当邻居节点收到追踪消息后, 将追踪消息里的信息和本地存储的信息进行比较, 判断攻击报文是否经过自己或由自己转发过。如果是的话, 该节点就继续将追踪消息发送给它的所有邻居节点, 并向 DC 发送汇报消息; 如果自己不在攻击路径上, 仅仅向 DC 发送汇报消息, 对追踪消息不进行转发。该过程一直进行到追踪至攻击源或 CITRA 网络的边界。

在 CITRA 网络中, DC 是管理中心, 它负责接收所有节点发送的汇报消息, 从而获得整体的入侵情况, 重构出攻击路径, 并且反馈响应指示给各个节点, 令其终止不合适的响应动作或加载新的响应措施。

CITRA 的优势在于它是一种分布式的入侵追踪技术, 并且它的追踪不受时间限制, 即使在攻击结束后的一段时间也可以进行, 增强了它的适应性和灵活性。由于它的大部分动作都是自动进行, 因此不会给管理员带来过多的负担。但是它也存在缺陷, 即在 CITRA 管理域内所有的系统都必须按照 CITRA 框架设计和运行, 以确保消息的相互流通和信息共享, 一旦处于攻击路径上的某个系统不兼容, 追踪就无法进行。

### 3. 休眠水印追踪 (SWT, Sleepy Watermark Tracing)

SWT 也是一种基于主动网络的入侵追踪技术。在 SWT 系统中, 为了有效地追踪, 必须通过观察离主机最近的路由器或网关来监控主机, 这类网关被称为守护网关。而离主机最近的、负责转发入流量的守护网关称为入流守护网关, 负责转发出流量的称为出流守护网关。一个主机可以有不止一个的入流或出流网关, 守护网关集合为一台主机的入和出流守护网关总和。对任意守护网关集合  $G$ , 把凡是守护网关为  $G$  的子集的那些主机定义为  $G$  的被保护主机。定义连接链中主机之间的连接为跳, 用  $\langle \rangle$  表示。一跳可以包括多跳, 或物

理网络中的多个连接，由以下五个元素描述：<协议号，源地址，源端口号，目标地址，目标端口号>。这样追踪问题就被定义为发现并排序在入侵路径上的主机的守护网关，或者（同等地）发现入侵路线上的跳。

SWT 框架包括两个部分：SWT 被保护主机和 SWT 守护网关。在信任模型中，SWT 被保护主机只有一个守护网关，并且它维护一个指向其网关的指针。每一个 SWT 守护网关保护一个或多个主机并维护一张保护主机的列表。在一台 SWT 被保护主机上的 IDS 和 SWT 应用程序也是 SWT 支持的组件，IDS 是 SWT 追踪的最初发起者。

SWT 的核心包括三个交互的部分：睡眠入侵响应、水印综合和实时追踪。睡眠入侵响应负责接收来自入侵检测系统的追踪请求，协调事实追踪和跟踪信息；水印综合的出和入水印连接；实时追踪负责协调网络的不同部分来协同追踪入侵源。通常睡眠入侵响应和实时追踪驻留在被保护主机上，当入侵检测系统发出追踪请求时，睡眠入侵响应就调动水印综合应用程序和实时追踪模块来初始化从本机到守护网关的实时追踪。在 SWT 守护网关上，实时追踪模块负责接收追踪请求并向水印综合提供水印。水印综合的出连接和入连接的情况，反过来也向实时追踪模块提供下一跳的 SWT 网关信息。一旦 SWT 守护网关发现下一跳的信息，实时追踪将向初始的主机发送这部分的追踪信息并通知下一跳的 SWT 守护网关开始水印追踪。

水印是一小块信息，用于唯一地标志一个连接。水印属于应用层，易于嵌入并检索，对网络的一般用户不可见，还必须能够综合多个连接并保持不变。为了证明连接的相关性，必须对出流量和入流量进行相关性分析，把水印作为相关性分析的基础。于是相关性分析就简化为扫描那些具有相同水印的出、入流量。当一个 SWT 守护网关扫描入流量时，它就把流量水印登记起来，当它扫描出流量时，它就把具有相同水印的流量匹配起来。

SWT 的优点在于：在没有检测到攻击的情况下，SWT 不会给网络造成任何负担，处于休眠状态。在攻击被检测到的时候，系统被激活，攻击目标会向网络连接注入水印（标记），唤醒攻击路径上的中继路由器，并与之协作进行追踪。不足之处就在于 SWT 只能工作在主动网络中，仍只是适用于未加密的连接，不适合目前绝大多数的网络情况。而且一旦一个老练的入侵者在知道使用了 SWT 系统后，会删除已被注入的水印，如此，追踪系统又将失灵。总之，到目前为止对于报文水印的研究还十分缺乏。

#### 8.5.4 面向连接链追踪技术的性能比较

基于主机的连接链入侵追踪，通过审计和监视经过主机的网络报文，以及与其他主机交互，来完成入侵追踪功能。在追踪性能上，主要计算、监视和交互工作都在主机完成，这就依赖主机对入侵的发现和入侵事件具有相关分析性能；在时效性上，发现入侵到追踪到入侵源的时延主要是端节点完成追踪需要的数据量，以及处理的计算时间和主机之间的通信时间，在追查入侵源的时限上有较好的事后追踪能力；在健壮性和安全性上，



也主要依赖所在网络的健壮性和安全性；在扩展性上，由于主要是主机之间的通信，因而具有良好的可扩展性。

基于网络的连接链入侵追踪，在网络合适位置上安插代理或嗅探器，把网络连接成一个整体，把这些代理或嗅探器监测到的信息进行分析或它们之间通信来完成入侵检测和追踪。在追踪性能上，主要计算、监视和交互工作都在代理或嗅探器上完成，这主要与这些代理或嗅探器对入侵的发现和入侵事件关联分析性能直接相关；在时效性上，发现入侵到追踪到入侵源的时延主要是代理或嗅探器上完成追踪需要的数据量，以及处理方法的计算时间和代理或嗅探器之间通信所有的时间，在追查入侵源的时限上有很好的事后追踪能力；在健壮性和安全性上，除了主要依赖所在网络的健壮性和安全性外，还很大程度上依赖安插在网络上的代理或嗅探器；在扩展性上，外加设备的机制具有良好的可扩展性。

基于主动网络的连接链追踪可以灵活部署追踪算法和协议，适应网络环境和攻击特征的改变。由于主动网络侧重包转发处理的定制特性，所以主动网络技术适合于对包处理的反向追踪方法。主动方法可以积极干扰追踪流量或连接，借此分析连接关联，减少追踪时间和开销。但是它需要路径上的主机全部部署为主动节点并且追踪速度缓慢。如主动休眠水印追踪通过目标主机向网络中入侵链注入一个水印，唤醒自身追踪功能并和中间路由器配合，但它并没有在具体的主动网络平台上实现，并且扫描位置不确定的水印开销较大。

在运行性能上，面向连接链的追踪技术的运行性能比较见表 8-2。

表 8-2 面向连接链的追踪技术的运行性能比较

技 术 方 法	网络流 量负担	中间设 备负载	管理 负担	分布式 能力	处理器内存 占用情况	事后追 踪能力	扩展 性
基于主机的连接链追踪	高	低	高	极好	低	较好	较好
基于网络的连接链追踪	高	低	高	极好	低	很好	较好
基于主动网络的连接链追踪	高	低	高	极好	低	很好	较好



# 第 9 章

## 网络空间作战的指挥控制

明晰的指挥控制关系对确保及时、有效地适用部队是非常关键的。信息化时代的网络空间作战，其指挥控制发生了翻天覆地的变化，其指挥流程、指挥活动、指挥层次、指挥跨度、指挥决策等方方面面与传统作战都有很大不同。在通常情况下，网络空间作战需要战区作战和全球作战之间的协调，需要在联合作战指挥控制理论体系中，建立与其配套的网络空间作战指挥控制理念，创造一个动态的指挥控制环境。为了使作战指挥控制理论更加系统、配套和全面，需要把网络空间作战集成到部队的作战概念、详细的计划、决策和命令，以及具体的联合进攻和防御作战中，以便实施协同和有效的作战。为此，需要对网络空间作战的指挥控制进行详细的探讨和研究。

### 9.1 联合作战下的指挥控制

#### 9.1.1 基本概念与内涵

##### 1. 相关概念

(1) 联合作战，就是各军兵种的力量，为达成一致的作战目的，在联合指挥机构的统

一指挥下，通过指挥、控制、通信、计算机、情报及监视与侦察系统（C<sup>4</sup>ISR），协调一致、相互支援、相互掩护，对敌共同进行的攻防作战，以实现功能互补，扬长避短，在多维战场空间形成综合优势。在信息化条件下联合作战的主要特点是：战场空间多维一体、信息系统互联互通、参战力量多元融合、指挥控制精确高效、综合保障精确集约、作战思想协调统一。

（2）作战指挥，是指指挥员及其指挥机关为达成一定作战目的，有效地运用现有资源的职责与权力，对所属部队作战行动进行的运筹决策、计划管理、组织领导、协调控制活动，力图实现人与武器技术装备的最优化结合，形成整体作战能力。其内容涉及作战指挥规律、作战指挥原则、作战指挥活动、作战指挥环境、作战指挥体制、作战指挥机构、作战指挥方式、作战指挥手段、作战指挥人员、作战指挥保障、作战指挥艺术、作战指挥训练等。按作战类型分为进攻作战指挥和防御作战指挥；按作战范围和层次分为战略指挥、战役指挥和战斗指挥；按作战力量构成分为联合作战指挥、军种作战指挥和兵种作战指挥。

（3）指挥系统，由指挥员、指挥机关和指挥手段等要素，按一定的组织形式构成的具有组织指挥功能的有机整体。通常依据体制编制或作战编成及指挥关系建立。按层次分为战略指挥系统、战役指挥系统和战斗指挥系统；按军兵种分为联合指挥系统、军种指挥系统和兵种指挥系统。

（4）指挥信息系统，以计算机网络为核心，由指挥控制、情报、通信、信息对抗、综合保障等分系统组成，可对作战信息进行实时的获取、传输、处理，用于保障各级指挥机构对所属部队和武器实施科学高效指挥控制的军事信息系统。按指挥层次分为战略指挥信息系统、战役指挥信息系统和战术指挥信息系统；按军种分为陆军指挥信息系统、海军指挥信息系统、空军指挥信息系统、火箭军指挥信息系统和战略支援部队指挥信息系统。

（5）控制，是施控者影响和支配受控制者的行为过程，掌握住对象不使其任意活动或超出范围，是一种有目的的活动。

## 2. 指挥控制的概念与内涵

### 1) 指挥控制的定义

指挥控制是指指挥员及其指挥机关对部队作战或其行动掌握和制约的活动，是对兵力资源的统帅、组织、领导、指导、决策、命令和筹划，以及对人员、装备、资源的有效使用和协调控制的过程和结果的描述。

指挥控制包含三大要素：一是人，包括指挥员及其所属、配属部队；二是技术，即完成指挥控制所需的设施、设备、通信等；三是处理过程，即收集和分析信息、决策、组织资源、规划、传达指令和其他信息、协调、监测结果、监督执行以及其他一系列活动。这三者有机地结合在一起构成了指挥控制。

一体化联合作战指挥控制是指在联合作战准备与实施中，联合作战指挥员及其指挥机关，按照总的企图和统一计划，以一体化指挥信息系统为依托，对参战诸部队联合作战行

动的组织领导活动。与传统的指挥控制相比，一体化联合作战指挥控制具有“信息主导、要素联合、统一筹划、协调同步”的本质特征。

## 2) 指挥控制功能

信息作战指挥控制功能包括：(1) 将政策行动纲领转变为军事命令，确保在战场中不违反政策；(2) 持续地对当前军事态势进行评估；(3) 制定决策和计划；(4) 将计划传达给下级，确保他们协调行动；(5) 预测未来可能出现的需求；(6) 执行战略作战，如心理战；(7) 提供包括技术和行政上的各种专门服务。

一切社会活动都有其明确的目的。军队中的指挥控制，其直接目的就是提高部队整体效能，间接目的就是夺取作战胜利。指挥控制的功能是具有层次性的，在不同级别的作战当中，指挥控制具有不同的功能。战略层面的指挥控制，关注的是如何通过确定组织目的、属性和最终性能来塑造一支成功的军队；战役、战术层面的指挥控制关注的是为了完成特定的使命目标意图，应该如何运用组织的资源（人力、体制、物资）处理好各种关系。

## 3) 指挥控制内容

概括起来讲，指挥控制内容大体分为四个部分：(1) 对各种武器装备的指挥控制；(2) 对各级战斗人员的指挥控制；(3) 对大量战场信息的指挥控制；(4) 对作战实体间的交互作用及指挥控制中决策和执行这两个过程间交互作用的指挥控制。

## 4) 指挥控制方式

指挥控制方式是指指挥者与指挥对象之间发生关系、进行职权分配的方法和形式。在平台中心战条件下，指挥控制方式大致可分为集中指挥、分散指挥、按级指挥、越级指挥等。在网络空间作战条件下，指挥员对指挥方式的选择与运用也更得心应手，将会出现动态分权式指挥、网络节点式指挥和虚拟游动式指挥等新的方式。

## 5) 指挥控制系统

指挥控制系统是指保障指挥员和指挥机关对作战人员和武器系统实施指挥和控制的信息系统，是指挥信息系统的核心。信息化条件下，指挥控制系统能够迅速地通过多传感器融合、多频段合成、战场环境与态势感知分析、网络化多站信息公用共享等方式，实现复杂战场环境下的目标探测与识别、战场态势与威胁评估、指挥控制等功能，大大提高了情报获取、传递、处理和利用能力，加快了作战指挥决策的时效性，增强了作战指挥的科学性，充分发挥武器装备系统的整体作战效能。

## 6) 指挥控制技术

指挥控制技术就是利用计算机、网络等手段，保障指挥员及其指挥机关对所属部队和武器装备实施有效指挥和控制的技术，包括态势生成技术、决策支持技术、计划协同技术和同步控制技术等。

## 7) 指挥控制的作战域

将指挥控制中的信息流所涉及的区域划分为四个作战域：物理域、信息域、认知域和社会域。

**物理域：**兵力管理、机动、打击、保护等军事行动所涉及的实际区域，指挥所设施、作战平台、目标和战场实际环境，包括陆、海、空、天。

**信息域：**提取、加工、处理和存储信息的区域，在此域内，信息可以共享，作战意图和计划被传送，包括信息系统、处理设备和传输网络等。

**认知域：**完成感知、认识、知识、经验、理解、推断和决策等认知活动的区域，认知域存在于决策者和参与者的头脑中，同时也是价值、信念和决心的驻留之地。

**社会域：**组织、指挥控制体系、个体和个体、个体和设备之间关系存在的区域。涉及指挥控制过程、作战单元之间的交互关系、部队组成结构和条令等。

可以说，一体化联合作战指挥控制系统依赖于信息域，决胜于认知域，协同于社会域，作用于物理域。

## 9.1.2 指挥控制过程

指挥流程强调了指挥相关的工作流程，是由一系列相对明确、先后有序、首尾衔接的若干阶段或基本环节所构成的一个特定的过程。指挥控制过程示意图如图 9-1 所示，从图 9-1 (a) 中可知，基本指挥过程有 8 个步骤。

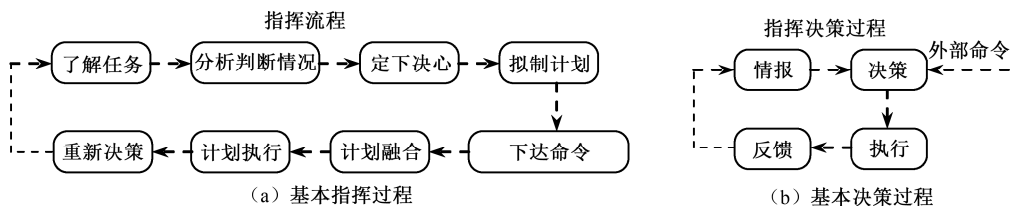


图 9-1 指挥控制过程示意图

(1) 了解任务：了解指挥所指挥的本级部队当前所要完成的作战任务。

(2) 分析判断情况：由上级情报信息子系统获取，或通过同级指挥所系统共享的敌情、战场环境、目标性质等数据进行分析与判断。

(3) 定下决心：明确敌情、我情、战场环境，分析己方可以使用的作战单元和武器装备，根据决策的原则和限定性条件，进行决策，定下决心。

(4) 拟制计划：指挥员确定满足作战规则和作战效率要求的作战单元选择、阵地部署，打击方式选择等的优化方案，拟制作战计划。

(5) 下达命令：将作战命令下达到下级执行。

(6) 计划融合：融合不同级别的上级命令，得到本级的行动计划。

(7) 计划执行：下级单位执行命令。

(8) 重新决策：下级单位命令执行完毕后，停止以后或不能执行的命令，重新进行决策。

针对任何一项指挥内容所进行的决策活动，产生一定的指挥决策过程。基本决策过程如图 9-1(b)所示，在一个决策周期内，收集情报，将决策转化为行动执行的命令，命令执行后的行动效果作为下一步反馈，去完成新的决策。

表 9-1 是各指挥控制步骤的输入与输出，为参谋机构提供了一种职责和活动列表，阐述在各个阶段应当做些什么，以及怎样做的问题。

表 9-1 各指挥控制步骤的输入与输出

步 骤	输 出	输 入
(1) 了解任务	本级初始态势感知	从上级指挥所获得任务或由本级指挥所分配任务
(2) 分析判断情况	初始化作战意图、作战计划的指导信息，初始情报侦察计划，初始机动	上级指挥所的命令、计划，上级指挥所的情报态势感知
(3) 定下决心		初始作战意图、作战计划的指导信息，初始情报侦察计划，初始机动
(4) 拟制计划	作战行动序列的表达和概括，初步决心和作战计划指导信息	更新的任务，初始作战意图和情报侦察，更新的态势感知
(5) 下达命令	初步决心和作战计划指导信息	
(6) 计划融合	决策矩阵命令（优化的行动过程序列，更新的决心意图，高回报的目标清单）更新的情报、侦察	更新的决心意图和作战计划指导信息，敌方行动过程序列、作战行动序列的表达和概括，比较评估方法
(7) 计划执行	供执行的命令	作战计划命令
(8) 重新决策	转到步骤（1）	

在系统中，情报参谋综合来自上级情报部门、下级情报部门、传感器等情报源的情报信息，分析判断后得出情报结论，存储备查或通过指挥自动化系统的文电传输分系统分发到有关指挥员的席位上，供指挥决策使用，并报上级指挥所和通报友邻部队及下属部队。后勤参谋统计汇总下属各作战部队的后勤资源状态，及时调整和补充后勤资源，保障后勤供应，并把相应的后勤资源状态报告给作战参谋。作战参谋根据上级下达的任务，综合各种敌情和己方的后勤资源状态，参考各种备查的作战基础数据，制订相应的作战计划，并发布至相关部门和下级作战部队。一种典型的某一级指挥节点的指挥信息流程图如图 9-2 所示。

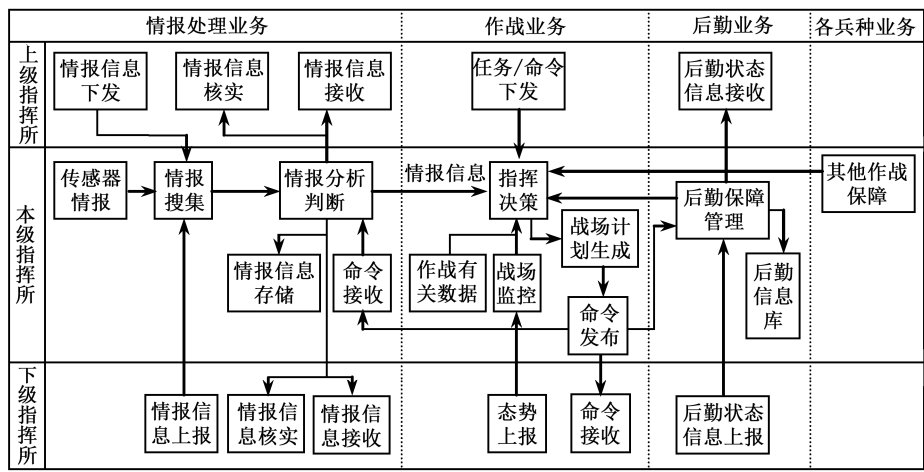


图 9-2 某一级指挥节点的指挥信息流程图

### 9.1.3 指挥控制的系统架构

作战指挥控制能力主要建立横向及纵向指挥控制机制，根据战场基本信息和辅助决策方案及时有效地下达作战指令，控制各作战平台实施有效对抗。

#### 1. 系统框架

信息化指挥控制的系统框架应从作战需求、系统需求、技术支持三个方面考虑。典型信息化指挥控制系统组成如图 9-3 所示。指挥控制系统由信息处理、辅助决策、指挥控制、人机交互四个分系统和数据库组成，再通过网络互联互通，采集侦察与态势感知系统的信息，指挥员直接与指挥控制系统交互，指导对抗和作战。

#### 2. 软件体系结构

为了实现大规模系统的动态集成，实现软件系统的开放性、可移植性和互操作性，基于软件总线的分层开放的构架体系已经成为大型系统构建的首选方案。

软件总线体系结构是借鉴计算机硬件技术而提出的。软件总线，是指面向对象的为多种计算机语言编写的多个、多种类型的软件功能部件服务的一组虚拟的数据信息传输线。这组虚拟的数据信息传输线是软件，是一组通用的标准集成软件功能部件的接口界面，是计算机操作系统与各种集成功能部件之间或集成软件功能部件之间进行数据传输与联系的虚拟公共通道和接口界面。指挥控制系统软件体系结构如图 9-4 所示。

核心层包括操作系统、数据库管理系统和其他支撑软件。



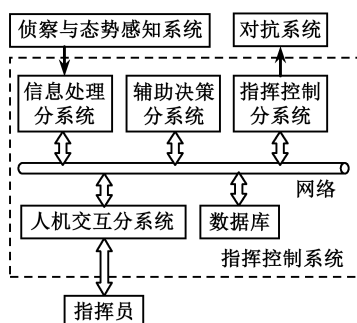


图 9-3 典型信息化指挥控制系统组成

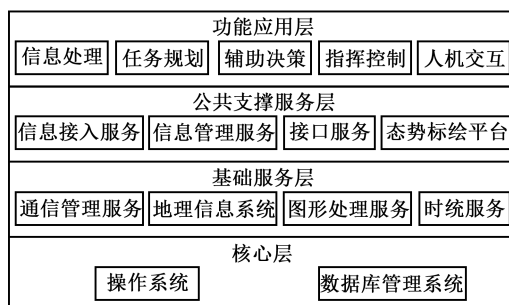


图 9-4 指挥控制系统软件体系结构

基础服务层由通信管理服务、地理信息系统、图形处理服务、时统服务等各种基础服务组成。

公共支撑服务层基于基础服务软件之上，为信息系统应用功能提供关键业务支撑。主要由信息接入服务、信息管理服务、接口服务、态势标绘平台等公共支撑服务软件构成。

功能应用层由直接面向用户的应用软件构成，主要由信息处理、任务规划、辅助决策指挥控制、人机交互等应用软件组成，为系统提供专用应用支持。

### 3. 软件系统基本模型

根据信息化指挥控制行为功能需求，信息化指挥控制系统软件组成的基本模型模块包括信息处理功能模块、任务规划功能模块、辅助决策功能模块、指挥控制功能模块、战况重演功能模块、人机交互功能模块，以及其他基础服务功能模块。指挥控制系统软件组成基本模型如图 9-5 所示。

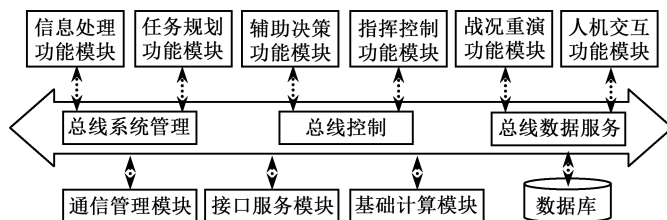


图 9-5 指挥控制系统软件组成基本模型

信息处理功能模块完成各路情报信息综合处理、目标航迹辨识、多目标分选及威胁等级判别、战场态势威胁评估等功能，主要包括信息综合处理、信息融合等软件构件。

任务规划功能模块根据上级指挥所的作战命令和作战区域特点，完成布阵计算，对系统内各分系统的作战任务进行规划和部署，主要包括作战资源分配服务、布阵计算服务等软件构件。

指挥控制功能模块，即指挥控制和作战辅助决策功能模块，完成战时系统的干扰资源管理、分配，提出指挥决策建议供指挥员参考，形成指挥决策方案，发出控制命令。主要

包括设备管理服务、辅助决策、指挥控制等软件构件。

战况重演功能模块完成历史作战过程回放、重演等功能。包括作战数据管理服务、战况重演控制、战况回放等软件构件。

人机交互功能模块完成战场态势信息实时显示，提供人机交互接口等功能，包括战场态势图形显示、数据信息表格显示等软件构件。

其他基础服务功能模块主要完成对上对下接口服务、通信管理服务、基础计算服务等功能。

## 9.2 网络空间作战指挥控制的战术技术要求

### 9.2.1 网络空间作战指挥控制的基本概念与属性

#### 1. 基本概念

网络空间作战指挥控制是指网络空间作战指挥员和指挥机构对网络空间作战力量（如网络战士）的组织、筹备和部署，以及在作战过程中为适应对手、环境、作战节奏和进程变化而实施的调整和控制。显然，网络空间指挥控制包含作战之前力量的筹划部署和作战过程中的协调控制两个环节。网络空间指挥控制的本质，是网络空间作战指挥员对网络空间作战力量的有效驾驭。这种驾驭表现为网络空间作战指挥员所具有的权威性，是建立在指挥员对作战多要素的客观认识和指挥员对作战力量连续可靠的指挥和控制基础上的。网络空间指挥控制的根本目标，是实现制信息（包含网络）权和网络空间作战力量作战效能的最大化，最大限度地发挥网络空间作战力量的战斗力，提高网络空间行动效率。

#### 2. 基本属性

##### 1) 网络空间作战指挥控制的复杂度属性

网络空间作战指挥控制的复杂性突出表现在五个方面：一是网络空间力量的广泛性增强了指挥控制对象清晰掌握和有效控制的复杂度。只要掌握了信息系统的专门知识并能有效地闯入重要网络，就可以实施网络空间作战。二是网络空间手段的知识性增强了指挥控制手段高技术及其综合运用的复杂度。作战人员利用其丰富的电子技术知识，尤其入侵计算机网络和传播计算机病毒等技能和手段实施作战。三是网络空间的广阔性增加了指挥控制空间高维拓展和体系化的复杂度。网络空间作战是在电磁、信息和网络空间实施的作战，不受地域的制约，直接渗透到陆、海、空、天四个物理作战空间。四是网络行动的连续性增加了指挥控制的连续性和节奏有效控制的复杂度。网络空间作战几乎不受外界自然条件

的干扰,其作战时间具有连续性,是真正的全天候作战。五是网络空间行动的突变性增强了指挥控制应急反应和侦察预警的复杂度。网络空间攻击效果不受时间和距离的影响,具有瞬间到达的特性,作战行动往往在很短的时间内就能够完成。

## 2) 网络空间作战指挥控制的功能属性

为了实现网络空间资源运用效能的最大化,除遵循指挥控制的基本原则具有对应的基本功能之外,网络空间指挥控制要适应相应指挥控制的复杂度属性,具有时空转换功能、适应性功能和系统整合功能。

(1) 时空转换功能。时空转换功能是指对网络化的兵力系统和作战行动时间需求,可通过共享—合作—同步实现压缩。网络空间指挥控制的时空转换功能,反映了网络作战行动作战资源和作战空间的广泛性,通过空间的扩大可以换来时间的压缩。在实现空间和时间转换的同时,时空转换功能同步揭示了网络空间作战兵力放大的原则和实践途径。

(2) 适应性功能。指挥控制是兵力系统工作手段和系统运作机制等多要素的综合,系统运行机制包括系统进化、适应功能和自学习、自适应、自组织、自修复功能。在网络空间作战中,指挥控制的适应性是网络空间作战力量体系生命之源和作战组织的灵魂。

(3) 系统整合功能。系统整合功能是指系统的潜能与整合程度成正比。在现代军事系统中,整合是跨建制、层级、功能、时间和空间的集中表现,通常通过网络化手段和力量结构体系化融合来实现。在网络空间中,指挥控制的系统整合是指充分利用电子基础设施和信息网络技术形成的互通互连和互操作功能,不仅是指装备、人员、程序等作战资源的简单整合,更是对大系统和巨系统的结构组成的优势重组和整体提升,可以有效控制网络空间作战的资源、节奏和进程,提高指挥的精度和控制网络力量实施作战的精度和力度。

## 9.2.2 网络空间作战指挥控制的特点

网络空间作战指挥控制的特点,突出体现在以下几点。

### 1) 全域的一体化联合指挥控制

网络空间作战已超出传统作战的行动范畴,其作战区域遍布军事信息网、指挥专网、电磁网络和国际互联网等信息系统。网络空间作战指挥既要网络部队、电子对抗部队等专业军兵种进行指挥调度,还要针对陆、海、空、天实体空间的作战需求,利用网络空间为全域内的作战部队提供作战态势评估、行动协调控制和信息资源共享。作战一方基于信息栅格网络将分布在网络空间的各类传感器、虚拟分布的指挥节点和武器平台(系统)有机合成为精确、高效、全域覆盖的一体化指挥信息系统,可以将多维空间信息对抗、火力分布、侦查、预警情报等态势信息共享,实现对网络空间的物理域、信息域、认知域和社会域的有效作战和行动也需要一体化的联合指挥控制,一体化的多方配合。网络空间作战有其独特的“非完全军事”属性,地方信息技术机构及人员亦是网络空间作战力量不可或

缺的部分，对非军事人员的指挥、协调、引导和管控将直接影响网络空间作战的效果。因此网络空间作战指挥既要对军内资源进行协调和控制，又要对国家信息资源及可用力量进行统一调度和支配；指挥系统必须模块齐全、功能完备、系统集成和机制健全，指挥功能、指挥手段和指挥信息等高度融合，才能满足网络空间作战指挥的需要。

## 2) 全域的资源管理与力量调度

实现对分布在物理域、信息域、认知域和社会域的作战资源的全面管理，需要对网络空间的作战力量实现灵活的调度和按需集中。

## 3) 多尺度的网络态势生成

网络空间涉及范围广，作战行动关注领域差异大，为此需要针对不同作战方向和内容，形成不同尺度、不同方面的网络态势，并根据任务变化不断调整网络态势关注点。

## 4) 完备的作战筹划与预案拟制

由于网络行动都需要瞬时完成，任何意外事件的发生都可能导致不完备作战方案难以顺利实施，导致行动失败。因此，在网络行动筹划中，必须充分搜集目标情报，进行深入分析各种不确定因素，形成周密的行动计划和方案。

## 5) 全周期力量指挥与行动控制

网络行动的战略和战术筹划必须相互衔接，综合应用战术和战略行动。战术行动的成功需要在战略网络战的总体策划下进行，而不能任由特定部队随意组织实施。战略筹划可为战术行动提供大量的目标情报，并在目标系统中进行“潜伏”作战力量。战术行动是战略级网络行动的具体实施，包括平时的情报侦察、目标分析、武器研制和力量部署等。

## 6) 指挥决策层次高，自上而下高度同步

网络空间联合作战往往涉及国家主权、人权等敏感问题，因此往往会引起高层领导的关注。因此，网络空间联合作战指挥必须围绕政治行动，始终把握“国家利益至上”这个大局，坚决维护国家利益和社会安全稳定，避免某些西方国家抓住把柄，从政治上站稳反恐的立场。在网络行动中，网络作战指挥员与战士对行动的认知高度同步，才能实现战术和技术高度结合，形成智力优势，从而保证取得行动胜利。

## 7) 指挥控制快速准确、指挥协同性高

在网络空间中信息的产生和传递速度极快，若敌方预先植入或埋藏病毒和逻辑炸弹等，则可在短时间内造成大范围的损伤和破坏；从而使战争节奏加快，情况变化急剧，战机稍纵即逝，指挥反应时间大大缩短，争时间、抢速度、抓战机等将成为作战指挥的关键内容。网络空间实时的作战信息收集、传递、处理和显示，使指挥员能在千里之外的大屏幕上，直观、形象、实时地观察到反恐态势，能够确保作战指挥实现情况判断快、作战决

策快、计划组织快、协调行动快，从而提高作战指挥的实时性。同时，在网络空间作战过程中攻防速度快，指挥反应的时间很短。指挥信息系统中的辅助决策功能可以帮助指挥员根据战场实时的态势情况快速、准确地下定决心，全程掌控部队的作战行动，优化指挥流程，提高指挥效率，真正使各武器系统、指挥决策者、战场传感器网络有效耦合；各级指挥机构按照任务需求和上级指引进行判断和决策，指挥者与指挥对象能够根据战场数据链建设情况实时联通，形成对态势情况的一致性协同，分布式行动，指挥形式上虽然宽松，但协调程度却比以往更高。

#### 8) 指挥主体、权责按需动态分布

网络空间作战，参战军兵种多，力量构成多元，战场空间多维，在网络空间节点中分布的虚拟指挥节点根据作战任务需要都有可能变成其他力量单元的指挥主体。网络空间作战指挥主体要实现在指挥权责的灵活集中与分散，在顶层实施集权式指挥，在分布节点实时分散式指挥，基于任务要求实现指挥权力的动态调整。网络空间作战的指挥主体广泛分布于战场信息系统体系网络中，一个指挥主体遭到摧毁，其他网络节点可及时交接指挥权，避免指挥主体与对象间中断失联。分布式指挥主体能够极大程度地提高指挥过程的稳定性和自适应能力。利用网络信息系统，战场空间各作战单元可按需共享、定制态势信息，方便网络指挥节点中指挥决策者实时掌控战场动态，分担指挥压力，共享指挥权力，指挥权责实现动态分布式方向发展，指挥权责按照作战任务需要匹配，不同级别的指挥员承担对应的权责，能够最大限度地发挥指挥员的主动性，提高指挥效能和增强部队的机动性，避免指挥冗余。

#### 9) 指挥对抗具有“谋技”并举性

网络空间战场频谱、信息密集交织，参战力量多、分布广且动态协同配合难度大，要求指挥人员必须具备全面过硬的素质，以便能在多样化的舆情对抗中保持清醒认知，做到冷静判断、果断处置。网络空间作战指挥离不开信息技术的支撑，战争实践表明具有科技和信息资源优势的一方在网络空间作战行动指挥中可更好地发挥自身优势，在与敌方的指挥对抗中可抢占制信息权。这就要求网络空间作战指挥人员必须受过较好的教育培养，具有较高的专业素养，较高的专业门槛。

#### 10) 作战指挥系统组织结构更加扁平

作战指挥日趋信息化、智能化，指挥信息不仅要在纵向上上传、下达，在横向的共享公用也尤为重要，需要构建具有高度融通信息传递链路的指挥机构来满足网络空间作战指挥的需求。显然传统的“树状”结构已难以满足作战指挥的信息化和智能化发展的需要，建立层级精简和跨度增加的指挥结构已成为必然趋势。随着作战指挥系统组织结构的扁平化，指挥体系的综合效能也将得到提升。

## 9.2.3 网络空间作战的指导思想和原则

网络空间作战指导思想和原则，是网络空间作战特点规律的客观反映，是筹划与组织网络空间作战的基本理论依据，是指导与实施网络空间作战行动的基本准则。

### 1. 指导思想

网络空间作战的指导思想是：以全域网络态势感知为先导，以全方位的网络行动为基础，实施积极主动的网络空间作战并进攻关键目标，中断通信和补给线、扰乱敌方指挥控制系统、削弱敌军的军事行动、削弱敌方政治意志与社会凝聚力、形成对战争的全球感知；在全地域、全时域、全频域、全空域诱骗、阻止、抵制、消耗敌方，实施动态网络防御；以强有力的网络支援为网络行动提供支撑，以网络行动提升其他实体空间行动能力，保证国家和军队在网络空间的行动自由与优势。

网络空间行动的任务是：负责整个网络关键基础设施与核心资源，以及其他特定网络空间的建立、运行、管理、保护、防御和指挥与控制。

### 2. 作战原则

网络空间作战原则是组织和实施网络空间作战必须遵循的基本准则。研究确立正确科学、符合实际的网络空间作战原则，对有效组织实施网络空间作战行动具有积极的意义。

#### 1) 预先筹划和精确协调原则

预先筹划就是要预先出主意、想办法、订计划，为网络空间作战的开始做好充分准备。一是要立足联合战役全局，对联合战役网络空间各种作战力量、作战行动进行整体运筹和谋划。二是吸纳先进技术理念，较好地处理筹划过程中战术与技术的关系，将指挥官主观概念化，筹划活动与筹划团队的作战意识具体化，并与筹划活动融合为一体。三是有序高效的筹划流程要能够适应多样化的战争形态；四是筹划过程采用模块化结构搭建，各类配套业务流程相互支撑配合，在指挥控制、评估、情报和目标等业务流程的配合支撑下，实现对联合作战行动的持续和高效筹划。

精确协调涉及三个方面的问题：一是进行精确计划。在制订联合战役网络空间作战协同计划时，应考虑网络空间作战与其他联合战役作战的协同、网络空间各种作战协同、网络空间作战与作战保障之间的协同方面的问题，着眼发挥最大作战效应。二是精心协同。要精心部署周密安排，考虑多级、不同层面、不同军种、不同兵种的协同作战问题，还要考虑战略、战役和战术方面的协同问题。三是考虑组织协调、指挥协调、人员协调和网络协调方面的问题，担负起协同组织的任务。

#### 2) 提前组织和立体编成原则

提前组织，是指指挥员在联合战役发起之前，就开始着手组织网络空间作战行动。提前组织的内容主要是提前搭建组织架构、指挥体系和作战体系，组织网络空间侦察、网络

空间防护等工作, 尽早收集网络空间作战目标需要的参数, 提前制订网络空间攻击与网络空间防御计划, 组织对己方网络空间各种网络设施的防护。

立体编成就是围绕“网络任务”在不同空间编成满足作战任务需要的作战力量, 围绕“体系能力”的最大化综合编组各军兵种和网络空间作战力量, 围绕“全维对抗”科学配置各空间的作战力量。在实施立体编成中要注意把握以下三点: 一是要突出网络空间作战的核心要素、关键环节、重点方向、主要行动力量的编成与运用; 二是要科学编成, 做到软硬结合、攻防兼备、优势互补、梯次衔接, 网络力量与其他军兵种力量结构合理, 作战力量与保障力量比例适当, 作战能力与担负的作战任务相适应; 三是要统一筹划, 综合考虑, 不能顾此失彼。

### 3) 先行感知和全维监测原则

感知先行就是在网络空间作战行动中, 要以网络空间态势感知为先导, 通过积极主动的态势感知, 抢占网络空间作战先机, 争取作战主动权。主要途径通常有两点: 一是依靠绝对的作战能力优势争取主动; 二是依靠率先感知战场态势争取主动。态势感知是作战决策、作战指挥和作战行动的基础和前提, 要争取主动、抢占先机, 就必须先知先觉。

全维监测是网络空间作战指挥者在合理确定信息需求的前提下, 综合运用多种信息获取手段, 全面多维监视敌方网络空间, 不间断地获取敌方网络空间情报信息。贯彻全维监测原则, 科学组织各环节的信息活动, 综合运用探测(传感)器网, 实时掌握网络空间动态情况。

### 4) 统一指挥和全维行动原则

统一指挥是由网络空间作战特点所决定的。网络空间作战在战场构成上, 是陆、海、空、天、网五维一体。在作战行动上, 是侦、攻、防、控一体化行动。在作战力量上, 是军队网络空间作战力量和国家、民间团体网络空间作战力量的高度集成与融合。这些特点, 不仅决定了联合战役网络空间作战应统一指挥、统一控制、统一协调, 而且应视情分层控制, 充分发挥各级的能动性, 真正达成高度的统一。

一是在宏观上统一。就是要求局部行动服从和服务于全局行动, 贯彻总的作战意图。二是在时间上统一。在时间上统一进行作战控制和协同, 控制各种作战行动, 避免相互冲突, 形成整体合力。三是在专业力量上统一。

全维行动就是要在多维物理空间、多维虚拟空间对多类目标展开网络作战行动。对多类目标既有在实体空间的硬目标, 也有在虚拟空间的软目标; 既有战场上的军事目标, 也有社会上的民用目标; 既有传统的陆、海、空、天及电磁目标, 还包括人的心理及认知等。全维网络空间作战不仅体现在战场空间的全维, 而且体现在网络空间作战力量与其他作战力量的一体化, 还体现在多种作战行动的一体化。

### 5) 主动进攻和攻敌要害原则

主动进攻是指在网络空间作战中采取积极主动的攻势行动, 先敌侦察, 先敌部署, 先

敌攻击，抢占先机，争取主动，快速夺取网络空间优势和战场控制权。积极主动的网络进攻行动，要达成事半功倍的目的，还必须科学合理地选择进攻目标，主要应包括以下内容：一是以削弱敌方体系作战能力为网络攻击的首选目标；二是通过网络攻击瘫痪敌方指挥控制系统；三是在大规模作战行动开始之前通过网络行动削弱敌方的战斗意志和认知能力；四是通过网络行动切断敌方关键信息传输网络；五是通过网络攻击对具备战争潜力或对战争具有支撑作用的媒体、电力系统、金融网络等实施瘫痪；六是通过网络攻击削弱敌方的全球感知能力。

攻敌要害是指根据网络空间作战总体要求，集中网络空间作战主要攻击力量，对敌网络空间体系中的关键节点、主要网络平台、核心设施设备等实施重点攻击，力争攻其一点、毁瘫全网。贯彻运用这一原则，一是要确立攻击的要害目标，如联合作战行动中的公用网络平台、重要网络节点、信息系统中的要害部位、具备战略意义的国家网络设施、关键人物的认知等。二是要集中主要网络攻击力量于主要方向、重要时节、关键目标和主要作战行动。三是要瞄准薄弱环节，寻找敌方要害网络及设施的漏洞与薄弱之处，集中力量进行攻击。

#### 6) 动态防御和确保任务原则

动态防御是通过对整个网络系统的各项信息进行全面的监控，及时主动地采取实时动态的保护和防御措施。在网络诱骗方面，防御技术必须是主动出击的，不能够等待黑客的攻击，而是必须主动吸引黑客来进行攻击，可以提前设计好陷阱、诱饵等，引导黑客按照主动防御技术设计的游戏规则进行，及时获取黑客的信息，为研究破解黑客技术和反击做准备。在动态跟踪主动防御方面需要在防御的过程中实现全面的跟踪监测、文件监控、进程跟踪、击键捕获等。

在网络空间作战中贯彻运用动态防御原则，需要注意把握三点：一是网络防御与网络进攻协调一致行动。网络空间动态防御要将预案、感知、情报、传输、行动等进行高度综合，主动识别和分析恶意行为，并在恶意行为带来危害之前提示和启动攻击行动，挫败敌方的攻击企图，达到实时防御的目的。二是网络防御与其他作战领域的防御动态互补。三是网络空间技术防御与战术防御动态互补，技术决定战术，战术提升战力。

确保任务是指网络空间作战既要确保网络和基础设施安全，又要确保人员与信息安全，还要进行相关的勤务保障，但核心是要确保作战任务的完成，完成联合作战中的网络空间作战任务是一项最为基本的原则。其要义包括以下五个方面：一是围绕任务与其他各军兵种共同制订联合作战计划，包括任务清单、协同计划、支援保障计划、共同防御策略等。二是围绕任务确定各军兵种在联合作战中所需要使用的网络设施与资源。三是围绕任务在网络空间进行主动及深度防御。四是围绕任务与各军兵种实施联合攻击行动。五是围绕任务确定网络作战人员。

#### 7) 军民融合和整体制敌原则

军民融合是指在网络空间作战中，应充分依托国家信息网络基础设施，统一协调和充



分利用一切可资利用的网络资源,将军用、民用信息网络和人力与物力资源有机融合起来,构建起高度集成、军地一体,可以覆盖多维空间的战场信息网络及资源,形成优势互补。

无论网络进攻,还是网络防御,其领域已经远远超出了军事领域的范畴,在电力、电信、银行、金融、网络等广泛的民用领域都将是网络作战的目标,由此决定了必须走军民融合的道路。作战力量结构呈现知识化、精英化、平战一体、军地一体、兵民一体的柔性特征。对抗形式上,既有以军事集团为主体的战场网络空间作战,也有以组织团伙为主体的网络破坏活动,还有黑客个人自发的网络攻击行动。因此,在筹划网络空间作战行动时,指挥员应突破传统思维,应注重发挥地方的资源优势、技术优势和人才优势,与各级政府职能机关、信息安全部门和民间信息技术企业团体携手,统合运用各种力量,整合利用各种资源,形成多元互补的力量优势,最终形成网络空间军地一体、互为依托的有利态势。

整体制敌,就是使战役直属各种网络空间作战力量、各作战集团(群)网络空间作战力量组成一个有机整体,以整体作战力量的发挥去战胜对方。实现整体制敌须从三方面入手:一是坚决贯彻上级关于网络空间作战的指示和要求,着力使本级网络空间作战与上级网络空间作战形成一个整体。二是统一组织所属网络空间作战力量,统一部署,统一行动,形成整体合力。三是严密组织本级网络空间作战力量之间及与上级、友邻之间的协同,使各级、各类网络空间作战力量相互补充、相互配合,最大限度地发挥出整体威力,为夺得网络空间优势奠定坚实基础。

#### 9.2.4 网络空间作战指挥方式

网络空间作战指挥方式,是网络空间作战指挥员和指挥机关对网络作战力量实施指挥与控制所采取的方法和形式,其核心是在网络空间作战指挥活动中如何分配与使用指挥权。作为指挥员,应把握好各种指挥方式的特点、使用时机和要求,熟悉影响指挥方式运用的因素,在合理选择指挥方式的基础上,注重多种指挥方式的综合运用。

在网络空间作战指挥过程中,可以运用的指挥方式较为丰富,既有传统的集中式、分散式指挥方式,也有按级指挥、越级指挥、同步化指挥、网络化指挥和预案式指挥等方式。下面就对这7种基本作战指挥方式进行一一介绍。

##### 1) 集中式指挥

集中式指挥是网络空间作战指挥员集中掌握和运用指挥权,对所属作战力量进行集中控制、统一协调的指挥方式。这种方式不仅规定完成任务的具体方法和步骤,而且还对网络空间作战目标、作战过程、作战时机等进行精确控制。这就要求指挥员具有高度集中的指挥权力,包括组织计划、编组动员、兵力部署和调兵遣将等所需的权力。这种集中式指挥的优点是,便于网络空间作战指挥员统一指挥,形成整体合力,协调一致地完成作战任

务。主要不足是，指挥效率较低，对指挥手段依赖性强，不便于发挥下级指挥员的主观能动性。

集中式指挥的运用时机：一是对支撑敌战役级行动的指挥控制网、情报侦察网、战场通信网、预警探测网、卫星通信网等敌方敏感信息网络基础设施的攻击行动；二是为夺取网络空间优势，支援其他重大战役行动的网络空间作战行动；三是任务明确，敌情掌握详细时。这三种情况都可以运用集中式指挥方式。

## 2) 分散式指挥

分散式指挥是指指挥员只给下级明确意图和任务，由下级独立自主进行的网络空间作战指挥，是将指挥权力大部分下放给指挥对象的一种指挥方式。这种分散式指挥的优点是便于发挥网络空间作战下级指挥员的主观能动性，指挥效率较高。主要不足是对网络空间作战下级指挥员能力素质要求很高，同时不利于与友邻作战力量形成合力。

分散式指挥主要应用于网络空间作战防御以及网络空间作战情报侦察行动的组织指挥。分散式指挥的运用时机：一是当指挥对象执行作战任务变化快速而且频繁时；二是对敌情掌握特别是关键情况不甚明了，则给下级较多的临机处置权；三是当指挥控制信息网络遭敌破网成功，干扰到指挥员指挥的正常进行时。这三种情况则可视情运用分散式指挥。实施分散式指挥应做到建立监控体制、形成主动协调机制，并建立新的信息流程。

## 3) 按级指挥

按级指挥，是指按照网络空间作战编成的隶属关系逐级实施指挥的指挥方式。采取这种按级指挥方式，网络空间作战指挥员按照预先明确的递阶式指挥关系，上级只将命令下达给直接下级，下级将报告情况和请示汇报给直接上级。这种按级指挥的优点是，利于发挥网络空间作战各级指挥员的职能，指挥有序。主要不足是，指挥环节较多，指挥的时效不够。

## 4) 越级指挥

越级指挥，是指网络空间作战指挥员越过作战力量的直接上级对其实施指挥的指挥方式。采取这种越级指挥方式，是网络空间作战指挥员根据需要越过直接下级或数级向作战力量下达指令，被指挥的对象应直接向指挥者报告情况。这种越级指挥方式的优点是，减少了作战指挥层次，提高了指挥效率。主要不足是，对指挥手段依赖程度较大，对指挥者的工作能力要求较高。

## 5) 同步化指挥

同步化指挥，是网络空间作战上级和下级指挥员几乎同时组织指挥活动，展开指挥的指挥方式。采取这种同步化指挥方式，通常是网络空间作战上级指挥机构在受领任务后，在展开本级指挥的同时，迅速向下级下达预先号令、预告敌情等内容，下级接到预先号令后，随即展开本级组织指挥。此时，网络空间作战上级和下级指挥机构相互实时沟通，同

步展开指挥活动。这种同步化指挥方式的优点是,有利于提高网络空间作战指挥效率。主要不足是,对指挥手段的保障能力、指挥员的能力素质要求较高。

#### 6) 网络化指挥

网络化指挥是指网络空间作战指挥员依托网络信息系统,对各级指挥机构以及各种作战单元实施指挥的方式。采取这种网络化指挥方式,是网络空间作战指挥员依托各种类型的网络将分散配置在多维空间的作战、指挥和保障等要素链接在一起,依据信息流结构的特点来进行指挥控制。这种网络化指挥方式的优点是,网络空间作战指挥实时高效,能够有效调动战场上各类资源、形成体系作战能力。主要不足是,对网络系统的依赖程度和安全性要求较高,一旦关键节点遭敌打击,后果不堪设想。

网络化指挥的运用时机:一是执行特殊任务需要越级指挥时;二是作战力量多元、作战行动多样、协调关系复杂时;三是指挥员需要对网络空间作战全局行动有效掌控时。这三种情况下可采用网络化指挥方式。实施网络化指挥应做到以下几点:一是应综合控制好全局;二是综合协调好关系;三是灵活协调好各种力量;四是强化措施,辨别真伪。

#### 7) 预案式指挥

预案式指挥是指指挥员及其指挥机关根据担负的任务和网络空间作战行动特点,预先对可能的网络空间作战行动所采用的指挥手段、指挥方式、指挥活动等做出基本方案,作战过程中,根据网络空间作战行动选定指挥方案,并直接按照方案进行指挥的方式。

运用预案式指挥,指挥员有充分自由权,可根据预案,对情况及时做出处置,而不必先向上级报告情况等待指令,而后才做出处置,大大简化了指挥程序,缩短了指挥周期,从而提高了指挥效率。特别是当任务紧急、情况突变、反应时间十分有限时,运用预案式指挥,可及时明确战略目标和网络空间态势,明确上级指挥员的决心意图,下级指挥员可根据指挥预案和情况的变化发展,自主调控自己的行动或与相关力量和行动的主动协调,实施高度自主决断的指挥控制。

预案式指挥的使用时机:一是网络空间作战任务紧急、情况突变、反应时间短促时;二是当战场情况与设想情况一致时;三是指挥员指导协调各级网络空间作战过程中的指挥控制行动时。这三种情况下可采用预案式指挥方式。实施预案式指挥应做到以下几点:一是指指挥预案应周密;二是执行的网络空间作战任务和作战行动应与指挥预案设想的基本一致;三是强化安全保密措施;四是如果条件允许,战前可周密组织指挥预案的预实践,通过预实践演练进一步完善指挥预案,以提高预案式指挥的适用性和可操作性。

指挥方式的选择要根据作战样式、作战力量、指挥手段、人员素质、战场情况等因素确定。在网络空间作战中选择不同的指挥方式,将会对作战产生截然不同的效果。因此,在运用网络空间作战指挥方式时,应把握好各种指挥方式的特点、使用时机和要求,熟悉影响指挥方式运用的因素,在合理选择指挥方式的基础上,注重多种指挥方式的综合运用。

## 9.2.5 网络空间作战指挥关系

指挥关系是作战指挥中体现各指挥机构之间的权限、责任和相互联系的形式。明确网络空间作战指挥关系，目的在于理顺作战集团（群）之间、作战集团（群）与指挥机构之间、军队与地方之间的相互关系，明确指挥权力与义务，达到上级对下级实施顺畅的指挥和相互间协调一致的行动，是组织指挥有序运行的重要保证。

### 1. 垂直指挥关系

垂直指挥关系是一种上级指挥机构对下级指挥机构和作战单元具有直接指挥和控制的指挥关系，是一种相对固定的指挥关系。这是一种最可靠、关系最牢固、运用最广泛的指挥关系。形成一种垂直的、单向的、上下级的关系，先由上级指挥机构运筹、决策、计划，再逐级或越级下达控制命令，下级依据上级的指令展开作战行动，下级始终在上级的控制之下。它的主要优点是：上下联系十分紧密，任务容易理解和明确，执行命令坚决果断。垂直指挥关系包括了传统的隶属关系和配属关系。隶属关系，是按编制或作战编组构成的上下级指挥关系。配属关系是上级指挥员为加强所属某部队的作战能力，临时调拨所属其他部分建制部（分）队归其指挥，在配属与被配属部队之间建立的指挥关系。二者的主要区别：一是相互关系的紧密程度不同。隶属关系较之配属关系，其相互关系更加紧密，而配属关系则略显松散；二是所采用的指挥方式不同。隶属关系一般采用集中式指挥方式，而配属关系则多采用指导式指挥方式；三是指挥或指导的层次不同。隶属关系形成后，下级只接受本上级的指挥或指导，而在配属关系中，下级除了要接受新上级的指挥和指导外，还可以接受原上级的指导。

### 2. 平行指挥关系

平行指挥关系是一种松散的指挥关系，在网络空间作战中，除了最高网络作战指挥员对各网络作战单元实施统一指挥外，各作战单元在要共同完成一项作战任务时，作战过程中不可预见的情况将会随时发生，需要参与行动的各方根据上级总的作战意图，通过互相协作和协调来达成一致行动。由于是一种平行和平等的关系，无上下级关系，各作战单元只能通过上级事先明确或双方协商解决。平行指挥关系包括协作关系和协调关系两种。

协作关系是在没有上一级指挥机构指令的情况下，遂行随机作战任务时，横向间两个以上网络作战单元主动协作的一种关系。

协调关系是指根据上级指令，无隶属关系的两个以上部队、作战部门之间或军地之间，在进行相关作战活动中通过协商调整构成的协调与被协调的配合关系，是根据作战任务或工作职能所形成的一种关系。网络空间作战力量构成多元，网络空间作战行动整体性强，各网络空间作战力量之间相互依赖性大，建立起良好的协调关系，可进一步优化联合战役网络空间作战体系整体功能。由于协调关系的强制性相对较弱，无隶属关系，相互之间也没有上下级之分，不是通过行政命令而是通过平等协商而形成同层次、平行单位之间的密

切关系，达成协调各方统一行动的目的。

### 3. 随机动态指挥关系

随机动态指挥关系是指网络空间作战指挥机构建立后，网络作战指挥员与各作战单元指挥员以及作战要素之间的一种动态变化的关系。这种动态的指挥关系主要由两方面的因素引起：其一，力量的动态变化，带来指挥关系的动态变化。各种网络作战力量单元，根据作战需要进行效能融合，动态组合，在同一次战役或战斗中，隶属、配属、支援、协调、协作关系将动态变化；其二，指挥权的动态变化，带来指挥关系的动态变化。在栅格式信息网络的支撑下，将构成一个信息高度共享、指挥机构之间交叉融合、节点多路由互连的栅格式指挥体系，指挥权将在各个节点间依据作战信息流中心的改变而变化，造成指挥关系的动态变化。由于随机动态指挥关系的特殊性，在实施指挥时应着重把握以下几点：第一，要防止指挥关系出现真空；第二，要科学组合各种力量单元；第三，要充分发挥各作战单元的主观能动性；第四，要确保信息网络高度稳定，这是在网络空间战场实施高速、随机、动态协同的物质基础。

平行指挥关系与随机动态指挥关系的本质区别主要体现在两个方面，一是随机动态指挥关系中，在作战过程中的某一时间段，各作战单元会形成隶属、配属关系，也就是指挥与被指挥的关系；而在平行指挥关系中，各作战单元间始终是平等的关系，不会形成指挥与被指挥的关系。二是在随机动态指挥关系中，将会出现平行指挥关系中的协作与协调关系，且是动态变化的；而平行指挥关系中的协调、协作关系是固定不变的。

### 4. 支援关系

支援关系是无隶属关系的两个以上部队在共同遂行任务时所构成的相互协助、配合的关系。此种关系之下，担任支援任务的部（分）队并不脱离原建制，但被支援部队的指挥机构有权根据上级所明确的原则赋予其作战任务，提出行动要求。各作战集团（群）网络空间作战群之间、不同作战集团（群）网络空间作战群之间、各作战集团（群）网络空间作战群内部之间，可以根据受领的网络空间作战任务、作战行动的不同，确定为支援关系。

## 9.2.6 网络空间作战指挥控制流程

网络空间作战指挥控制流程如图 9-6 所示，它是实现各战略战术以及其他军事行动有效作战的基础，其目的是实现跨越整个电磁频谱的全域警戒、全域到达和全域作战能力，从而保护己方基础设施，指导军事作战，削弱或消除敌方军事能力。

下面对图 9-6 中内环的 6 个模块进行简要介绍。①采集与融合：网络空间态势获取和汇集。②存储与管理：保护态势数据，访问存储的数据，建立报告职责，确保网络各节点和各部队之间信息的通畅，解决使用不同手段获取信息的一致性问题。③分析与评估：确

定安全事件和计算相关的元数据，评估所有等级的对抗效果，测量行动和目标的进展，制定策略建议以推动形成后续的行动，分析和评估的相关信息可运用于充实、修正指挥控制中的决策辅助支持系统。④表示：精炼安全事件和相关的背景信息，形成全域的态势感知，维护对攻击的反应。⑤共享与分发：开发跨域的共享感知和机制以提交相关的数据给适当的团体。⑥应对：网络空间作战主要是规划和决策工作，确定局域和跨域的行动线路以减轻事件的影响，网络空间的应对有信息防堵、攻击、防护、反制和利用敌方信息系统等。

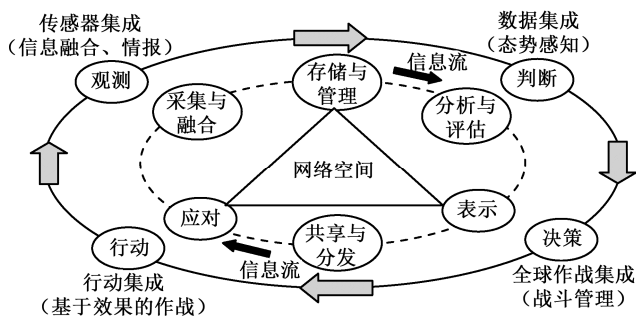


图 9-6 网络空间作战指挥控制流程

下面对图 9-6 中外环的 4 个模块进行简要介绍。①观测：采取观察、测量、传感器、数据库、情报系统等一切可能的方式获取网络空间中的信息，并对这些信息进行相关分析、组合和合成，产生关于网络空间战场环境多个目标的态势图。②判断：利用知识和经验来理解获取的信息，形成态势感知；再根据信息融合的结果，利用指挥控制知识库中的知识和各种信息对与任务有关的当前态势进行估计或对威胁进行判断；开发可选的方案。③决策：根据网络空间作战任务、目标和原则，进行资源分配和计划，选择行动方案，并加强管理。④行动：实施具体的网络空间作战行动，监控计划的执行情况，形成基于效果的作战。

网络空间作战指挥机构内部的指挥流程为：①传达网络空间作战任务和计划工作→②组织网络空间指挥和建立指挥信息系统→③判断网络空间作战情况→④制订详细的网络空间作战计划→⑤定下网络空间作战决心→⑥下达网络空间作战命令→⑦组织网络空间作战协调与保障→⑧控制、协调、展开网络空间作战行动→⑨作战效果的评估。

蓝军实施指挥控制的程序和方法涉及 6 个方面：①各种网络信息的收集→②网络信息的综合处理与决策→③网络作战方案的研究与制定→④作战方案的模拟分析→⑤指挥控制信息的分发→⑥命令执行情况的监控和作战效果的评估。

## 9.2.7 网络空间作战指挥控制系统技术体系

网络空间体系作战力量建设的目标是形成“联合、同步、高效、知识化”的网络空间

作战行动能力。其中,“联合”指网络空间作战力量能够与传统联合作战力量进行有效集成,互为支撑;另外,网络空间作战力量自身也需要加强各作战行动要素的协调发展,在强化攻防装备发展的同时注重作战指挥系统等的协调发展,形成具有较强适应能力的作战力量整体。“同步”就是改变现有人工为主的网络空间作战方式,实现各种行动要素的有效协作,使得整个行动过程更加优化而自动化,减少时间消耗,避免机械的行动过程,从而使得指挥员能够更加灵活地应用网络空间作战力量。“高效”是网络空间作战的必然要素,这里强调通过高效的作战辅助决策、作战计划自动生成等自动化方法,提高整个网络空间作战过程的效率。“知识化”体现了网络空间中人的主导作用,但这里更强调将人在网络空间作战中的“知识发现—知识创造—知识应用”等功能提炼出来,用于提高网络作战信息系统的知识化水平,从而既体现了人的作用,又发挥了“机器”的速度特点。

实现以上网络空间作战力量体系离不开与之相适应的军事信息系统。根据以上目标,设计出网络空间作战指挥信息系统的技术体系视图,如图9-7所示。该技术体系包括网络作战指挥控制系统功能组成、网络作战指挥控制系统技术和关键使能技术三个层次的研究内容。

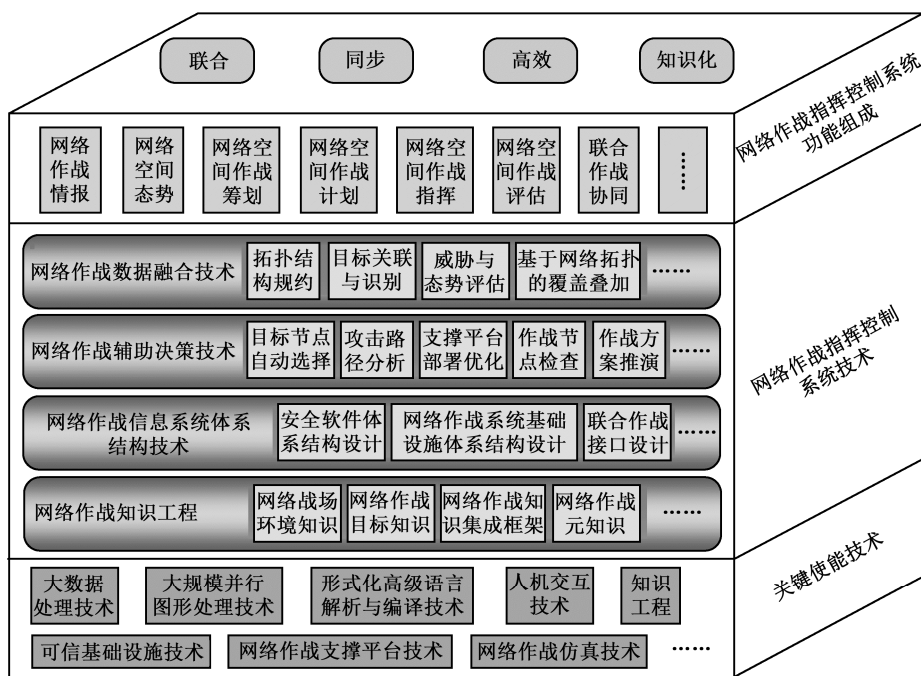


图 9-7 网络空间作战指挥信息系统技术体系视图

网络作战指挥控制系统功能组成是支撑网络空间作战行动指挥控制过程的各项要素,是形成网络空间作战体系的基本框架内容,涵盖了从网络作战情报、网络空间态势、网络空间作战筹划、网络空间作战计划、网络空间作战指挥、网络空间作战评估和联合作战协同等主要方面。

网络作战指挥控制系统技术是研制网络空间作战指挥控制系统的基础，包括网络作战数据融合技术、网络作战辅助决策技术、网络作战信息系统体系结构技术和网络作战知识工程等。网络作战信息系统技术与传统作战指挥信息系统技术方面存在较多区别。首先，由于网络空间是一个存在无限创造性的空间，因此数据融合方面需要处理更加海量、实时、多粒度、多源的数据。其次，在网络作战辅助决策方面，由于影响网络空间作战的时间周期缩短到秒级，甚至毫秒级，所以需要实现更加实时、高效、全面的辅助能力，而传统空间的辅助决策时间要求一般为分钟，甚至以天为单位。再次，网络作战信息系统的体系结构设计方面更加复杂，一方面需要考虑自身平台的安全性，另一方面该平台又不得不与对手的“危险”网络或主机发生连接。另外，该体系结构设计中还需要考虑如何与传统联合作战集成的问题。最后，网络作战知识工程是实现有效的网络空间作战能力的关键，网络作战涉及的知识体系更加丰富，小到一个字符串或一台主机和路由器，大到整个互联网，所有这些目标的相关作战知识都需要被掌握，并且需要综合应用这些不同尺度的知识内容。

制约网络作战指挥控制系统的关键使能技术包括大数据处理、大规模并行图形处理、形式化高级语言解析和编译、人机交互、知识工程、可信基础设施、网络空间作战仿真等技术。其中，大数据处理技术是支撑网络空间数据融合的基础，大规模并行图形处理是生成网络空间态势图的基础，形式化高级语言解析和编译技术是实现人的指挥活动直接翻译成机器可执行指令的基本语言，网络空间作战仿真是实现方案推演以优化行动计划的基础。

## 9.3 网络空间作战指挥控制的体制机制

网络空间作战指挥体系，是参与网络空间作战的各级、各类指挥机构按照网络空间作战指挥关系建立的有机整体，是网络空间作战体系的有机组成部分，反映各作战集团（群）内各级各类网络空间作战指挥机构的相互关系。在联合战役中建立与网络空间作战体系相适应的网络空间作战指挥体系，是确保对网络空间作战行动实施有效指挥，使各种网络空间作战行动形成有机整体，并与其他作战行动密切配合的前提。

### 9.3.1 网络空间作战指挥控制体系构建要求

作战指挥基本要素包括指挥者、被指挥者、指挥手段工具和指挥信息。指挥机构是指指挥活动的直接产生者，网络空间作战指挥机构的内部要素设置决定了指挥单元的功能与指挥活动的一般顺序，从而决定了指挥效能的生成过程。

构建网络空间作战指挥控制体系既要结合网络空间作战指挥的特点，满足己方作战指挥控制需求，符合己方网络空间建设的实际，同时，又应满足下列 3 项要求。



### 1) 有利于信息的交互贯通

未来战争中,计算机就是武器,夺取战争控制权的不是炮弹和子弹,而是网络里流动的比特和字节。在这个人为建造的虚拟信息空间——网络空间,任何指挥单元都离不开信息的收集与共享。信息融合程度影响着决策的正确性、控制的有效性和评估的合理性,进而直接决定着网络空间作战的胜负,这也是网络空间对作战指挥体系的客观要求。

### 2) 有利于行动的统一指挥

网络空间作战“牵一发而动全身”,一个作战目标可能需要多维作战力量的同时支撑,其作战任务复杂,覆盖域广,参战力量多元,军事对抗与非军事对抗并存。若无统一的协调、控制机制,将会出现各自为战、难以形成合力的问题。网络空间作战指挥体系的构建需满足对各种参战力量实施指挥的无缝接入和全局统揽,保证参战力量在统一的指挥下开展行动,实现高效的资源共享和精确的作战同步。

### 3) 有利于力量的协调控制

网络空间作战的参战力量不仅有网络侦察、进攻、防御力量,还有网络舆情对抗力量和实体打击力量。网络空间作战强调体系对抗、整体制胜,仅依靠单一的作战力量很难达到作战目的。网络空间作战指挥要通过高效的反馈沟通与协调控制,使各作战力量之间相互补充并形成具有高杀伤能量的有机整体,将分散的个体化作战能力融合形成一体化网络空间作战能力,实现信息与火力的高度融合。

仗怎样打,指挥体系就应怎样建,这是战争的客观要求。网络空间战场情况瞬息万变、作战节奏迅捷等特点,应按照“平战一体”的原则,依据现有指挥体制,建立平战结合的网络空间作战指挥体系,以便快速、高效地进行平战转换,避免战时因指挥机构筹建和职能转换带来的被动。构建网络空间作战指挥体系时,既应当有利于统一指挥、层次简明、高效稳定和控制协调,也应考虑到适应其高层次性、高技术性和军民一体性特征,确保建立的指挥控制体系有能力统合多种作战力量,确保指挥决策科学合理、可操作。

## 9.3.2 网络空间作战指挥能力构成框架与影响要素

深入分析网络空间作战指挥能力的构成要素及其之间的关系,对加强网络作战指挥能力建设、应对未来日趋严重的网络空间恐怖威胁具有十分重要的现实意义。

依据网络空间作战指挥的特点和任务需求,其作战指挥能力包括信息控制能力、指挥决策能力、组织计划能力、协调控制能力、快速反应能力、网络对抗能力、战效评估能力和指挥保障能力8种要素能力。这些能力既受指挥体制、指挥手段、理论体系和保障体系等外部因素的影响,也受内部各个构成要素的影响,其基本构成框架如图9-8所示。

(1) 信息控制能力，它是指网络空间作战指挥机构通过信息系统获取与控制情报信息的能力，包括信息获取能力、信息处理能力、信息共享能力和信息安全能力。其中：①信息获取能力是指收集网络恐怖活动有关信息的能力，其影响因素有情报侦察方法、信息获取技术和信息获取密度；②信息处理能力是指对收集到的海量信息进行识别、筛选、过滤、整理和融合的能力，其影响因素有信息处理速度、信息过滤能力、信息融合能力和信息识别水平；③信息共享能力是指在作战全过程中各级、各类指挥实体和作战实体按需共享恐情、己情、战场环境和作战意图等相关信息的能力，其影响因素有共享手段多样性、信息共享时效性和信息共享稳定性；④信息安全能力是指在作战过程中保证己方信息传输和安全利用的能力，其影响因素有信息备份能力、信息防毁能力和信息保密能力。

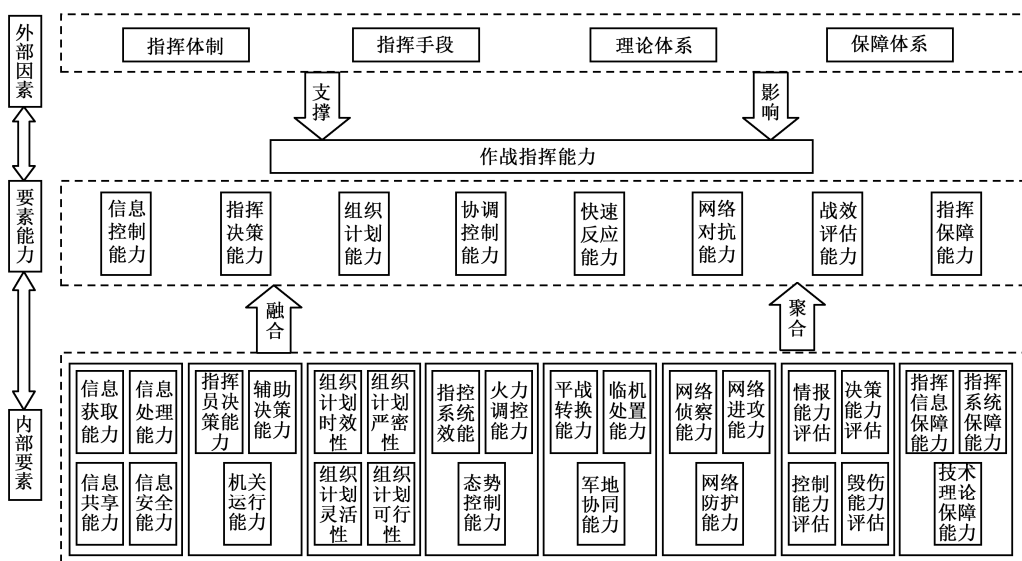


图 9-8 网络空间作战指挥能力基本构成框架

(2) 指挥决策能力，是指网络空间作战指挥员及指挥机关对作战行动进行运筹谋划和指挥决策的能力。指挥决策能力包括指挥员决策能力、辅助决策能力和机关运行能力。其中：①指挥员决策能力是指指挥员选择最佳网络作战行动方案的能力，其影响因素有指挥员素质、知识结构、指挥技能、指挥艺术和实践经验；②辅助决策能力是指参谋人员利用辅助决策系统，并综合各类情报信息，为指挥员提供科学合理的作战方案的能力，其影响因素有参谋人员能力和系统支撑能力；③机关运行能力是指作战指挥机构的各部门进行合理分工、协同，以保证指挥活动畅通的能力，其影响因素有统筹工作能力、人员配合程度和部门协调能力。

(3) 组织计划能力，是指网络空间作战指挥员及其指挥机关指导、联合各种网络空间作战力量进行作战准备和实施作战行动所进行的一系列预先设计和安排的能力。组织计划能力包括组织计划时效性、组织计划严密性、组织计划灵活性和组织计划可行性。其中：

①组织计划时效性是指在网络空间作战准备和实施过程中筹划各项工作的速度和效率,其影响因素有计划生成效率、统筹工作效率和计划变更速度;②组织计划严密性是指拟制网络空间作战计划、下达网络空间作战命令、组织协同各种保障等过程的严密程度,其影响因素有组织周密性、计划全面性和方案多样性;③组织计划灵活性是指根据恐怖袭击类型、手段和方式的不同,科学灵活地筹划网络空间作战行动过程,其影响因素有作战计划可变性、作战力量可变性和作战进程可变性;④组织计划可行性是指紧贴恐怖活动实际制定切实可行的行动方案,其影响因素有计划可操作性、内容具体程度和贴近战场程度。

(4) 协调控制能力,是指网络空间作战指挥员在定下作战决心和计划的基础上,根据网络空间恐怖袭击情况的变化,适时调整网络空间作战单元的行动,使其最大限度地发挥整体作战威力,最终达成网络空间作战目的的能力。协调控制能力包括指挥控制系统效能、火力调控能力和态势控制能力。其中:①指挥控制系统效能是指在网络空间反恐作战过程中指挥控制系统所发挥的功效,其影响因素有系统完善程度、系统反应时间、系统抗毁性和系统稳定性;②火力调控能力是指根据作战目标的毁伤效果,灵活地调整打击目标的能力,其影响因素有火力突击能力和火力支援能力;③态势控制能力是指根据战场作战态势的变化而及时地调整作战部署,以使作战行动配合得当,顺利达到作战意图的能力,其影响因素有作战行动准确性、协调行动有效性、调整部署及时性和掌握情况全面性。

(5) 快速反应能力,是指网络空间反恐作战指挥机构对突发的恐怖袭击或作战过程中出现的突发情况,迅速做出决策并临机处置的能力。快速反应能力包括平战转换能力、临机处置能力和军地协同能力。其中:①平战转换能力是指网络空间作战力量遇到突发事件时迅速转换成作战状态的能力,其影响因素有响应机制健全程度、平战转换速度和快速打击能力;②临机处置能力是指指挥员通过对恐怖袭击的动态情况和影响对象的分析,实现科学预判和正确处置的能力,其影响因素有科学确定突击时机、合理选择攻击手段、灵活运用攻击战法和高效指挥参战力量;③军地协同能力是指军队、武警、公安和地方联合作战力量相互支援、相互配合,应对突发事件的能力,其影响因素有军警、军民和警民协同能力。

(6) 网络对抗能力,是关系网络空间联合反恐作战成败的关键要素。网络对抗能力包括网络侦察能力、网络进攻能力和网络防护能力。其中:①网络侦察能力是指采用信息技术手段获取网络空间恐怖活动信息的能力,其影响因素有反恐情报侦察能力和恐怖活动发现能力;②网络进攻能力是指对敌方计算机网络、操作系统等进行攻击,达到阻止、削弱、破坏、摧毁或欺骗敌方网络行动权,确保己方网络空间行动权的能力,其影响因素有破坏通信能力、摧毁系统能力、病毒入侵能力、恐情解密能力和心理攻击能力;③网络防护能力是指依托信息技术基础设施,保护己方网络空间免受恐怖组织入侵破坏或受到攻击后快速恢复的能力,其影响因素有抗敌通信干扰能力、系统入侵预警能力、系统抗毁能力、系统恢复能力和作战保密能力。

(7) 战效评估能力,包括情报能力评估、决策能力评估、控制能力评估和毁伤能力评估。其中:①情报能力评估是指对反恐情报搜集的及时性、全面性和准确性,以及情报部门职能发挥程度等方面进行评估,其影响因素有情报部门工作效率、情报搜集全面性和情

报共享及时性；②决策能力评估是指对网络空间作战决策的合理性、科学性及指挥决策职能发挥程度进行评估，其影响因素有决策科学合理程度、系统辅助决策能力和决策效果反馈情况；③控制能力评估是指对战场态势的控制情况及作战指挥控制职能发挥程度进行评估，其影响因素有战场态势控制效果和兵力调配合理程度；④毁伤能力评估是指对己方计算机网络和指挥系统的受损程度，以及网络恐怖活动的受打击程度等进行评估，其影响因素有武器弹药效力、己方作战能力和敌方毁伤程度。

(8) 指挥保障能力，包括指挥信息保障能力、指挥系统保障能力和技术理论保障能力。其中：①指挥信息保障能力是指在网络空间作战过程中对情报、通信、网络、武器和设施等方面的信息保障，其影响因素有情报保障能力、通信保障水平、网络保障能力、武器保障能力和设施保障水平；②指挥系统保障能力是指对作战指挥系统进行防护和维护的能力，其影响因素有系统防护能力和系统维护能力；③技术理论保障能力是指与网络空间作战指挥活动有关的理论、技术保障能力，其影响因素有理论体系建设和技术保障水平。

### 9.3.3 网络空间作战指挥体系的设想架构

结合网络空间作战特点和作战指挥体系构建要求，立足军队现有指挥体系，依据网络空间作战力量编成和行动规律，构想网络空间作战体系的总体架构。

网络空间作战指挥体系框架如图 9-9 所示。由图 9-9 可以看出，在指挥结构上，网络空间作战行动是在军委联合作战指挥部的领导下统一部署展开，军委联合作战指挥部下设军委联指网络空间作战指挥部，军委联指网络空间作战指挥部下又设立战区联指网络空间作战指挥中心、战略支援部队网络空间作战指挥中心和军地网络空间协调中心。

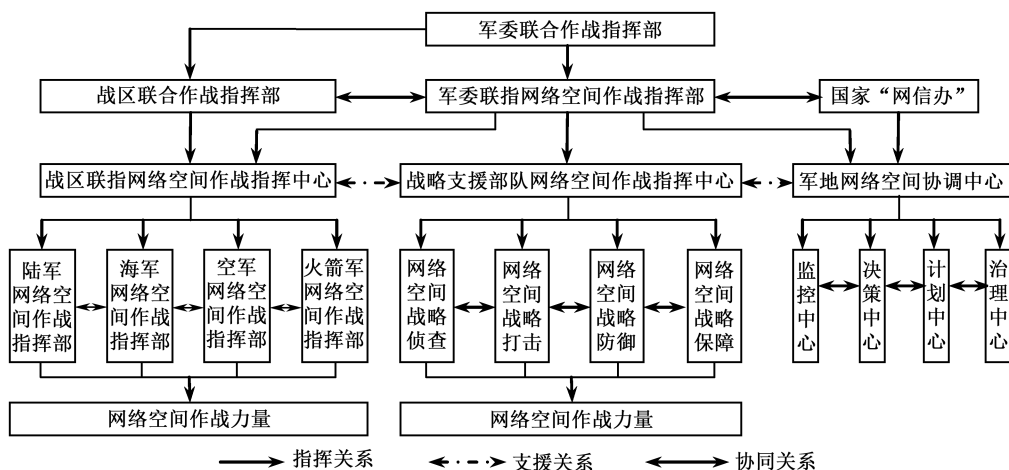


图 9-9 网络空间作战指挥体系框架

军委联指网络空间作战指挥部负责全国网络空间力量的统筹运用；负责全军网络空间作战行动的指挥、协调和控制，以及军队和地方的网络空间作战行动的协调与控制；并从整体上统一规划部署下属部门的作战行动，从全局出发确定方向、决心、目标和计划。其与战区联合作战指挥部和国家“网信办”处于同等地位，互为协同关系。

战区联指网络空间作战指挥中心主要是在战区联合指挥部的统一部署下负责战区网络空间作战的总体指挥。战区联指网络空间作战指挥中心下辖战区各军种网络空间作战指挥部，负责调配组织陆、海、空和火箭军各军兵种的网络空间作战力量；其与战略支援部队网络空间作战指挥中心、军地网络空间协调中心之间为支援和协同关系，前者为其提供战略信息和各类技术装备支援，后者为其提供非军事领域的信息资源和敌方有关动态，协助作战行动的开展。战区联指网络空间作战指挥中心主要负责对战役层次的网络空间作战行动进行指挥控制。在完成战略级网络空间任务时其处于从属地位，作战行动的指挥协调归上级统一部署；在完成战役级任务时其处于主导地位，当战区联合作战指挥部下达任务后，由本级组织作战决策、方案拟订、协调控制和作战评估等作战指挥活动。

战略支援部队网络空间作战指挥中心主要在战略层面上完成网络空间战略支援、战略打击、战略防御和战略保障等任务，并为战区联指网络空间作战指挥中心提供信息、技术和装备支援，支持其在战役层面上的作战行动。其与军地网络空间协调中心之间为协同关系，主要体现在信息的交流互通和相互支援，双方利用各自在本领域内的信息优势并形成优势互补，实现信息资源共享。其作战对象通常为国家或地区，作战行动方式主要是进行全方位、多角度和深层次的网络空间战略侦察和打击，破坏敌方整个网络的正常运行，对敌方军队和社会进行威慑；并在防御层面上指导全军网络空间作战防御力量部署，不断强化防御体系的安全性、稳定性和恢复性。同时，在信息资源的共享、技术装备的更新换代和战术战法的推陈出新方面，为全军各级网络空间作战指挥机构和力量提供技术和力量支援以及法规保障。

军地网络空间协调中心由军委联指网络空间作战指挥部和国家“网信办”统一领导，既有军方背景，又有地方身份，与战区网络空间作战指挥中心和战略支援部队网络空间作战指挥中心之间为支援和协同关系。其下设立监控、决策、计划和治理4个中心，主要针对对在国际互联网和社会舆论中产生重大影响的涉军、涉政和涉敏感问题，对网络舆论进行监督和引导，避免在舆论阵线上被敌方占有话语权；同时，引导军方和地方网络空间技术革新和装备研发成果交流。该中心由军方和地方网络空间科研机构和人员组成，主要负责收集作战行动中可能涉及的己方和敌方舆情、社情和民情，并反馈至战区和战略支援部队网络空间作战指挥中心，同时接收对方信息反馈，实现信息的高度共享。同时，协调、控制地方网络空间作战力量参与网络空间作战，使军地双方信息、资源、技术和力量共享。

### 9.3.4 网络空间作战指挥中心的结构

网络空间作战指挥中心设置的合理程度直接影响作战信息传达与反馈的效率，进而影

响网络空间作战指挥效能的发挥。根据网络空间作战力量的分布，结合网络空间作战指挥体系的构建原则，网络空间作战指挥中心应包括情报信息中心、网络攻击中心、网络防御中心、支援保障中心和外部协调中心，具体构成如图 9-10 所示。

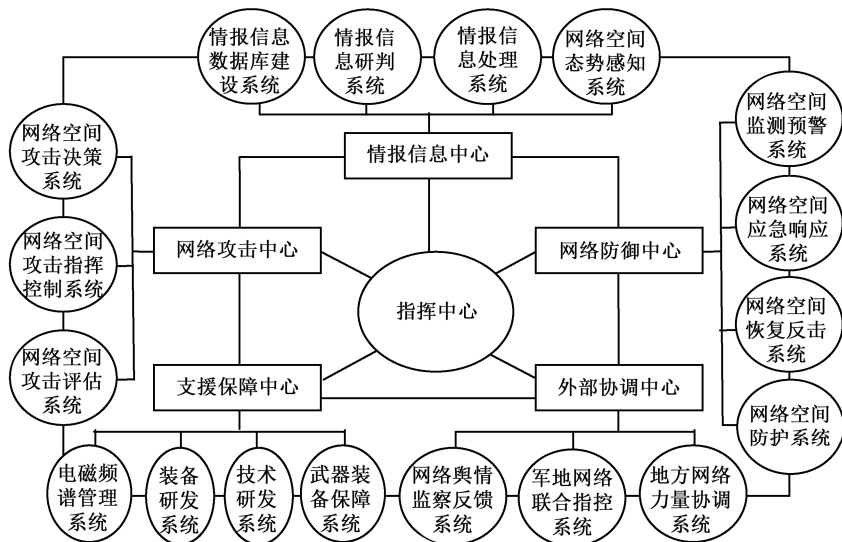


图 9-10 网络空间作战指挥中心构成

指挥中心是指挥机构的统帅部门，主要负责对下属的情报信息中心、网络攻击中心、网络防御中心、支援保障中心和外部协调中心进行统一领导和指挥控制，从全局上把握作战指挥进程和任务协调，接收情报信息中心的信息反馈，对网络攻击和防御中心下达作战决心和任务，规划支援保障中心的研究方向，针对网络空间作战任务需求协调外部协调中心进行作战支援。

情报信息中心主要利用人员、传感器和监控软件侦察，收集、分析和处理敌方、己方网络空间态势信息，并及时分发至各相关单元，如收集敌网动态、进攻进程和打击效果等与进攻作战相关信息，经分析、判别处理后，直接传递至网络攻击中心，辅助其开展下一步进攻行动。对于我方网络空间的异动、节点遭受破坏和不稳定等防御作战情况，则传递至网络防御中心并辅助其进行排查清理。同时，情报信息中心接收来自外部协调中心网络舆情监察反馈系统的信息，并整合各类网络资源辅助作战指挥机构进行决策；另外，建立战场情报信息数据库，并将收集的战场信息进行研究判断，形成以情报信息中心为核心的信息资源网络，以满足网络空间作战体系内各要素对信息的需求。

网络攻击中心由网络空间攻击决策系统、指挥控制系统和评估系统组成，接受情报信息中心提供的决策和行动指挥所需的战场实时环境、敌我双方网络空间的动态等作战信息，并与网络防御中心和外部协调中心相互合作、相互支援；支援保障中心为其研发、配备武器装备，并提供技术与作战保障。网络攻击中心负责对敌方网络空间的破网、渗透和控制，利用计算机病毒、电子干扰等手段对敌方网络空间进行干扰和破坏，并在必要时协同火力对敌方重要网络节点进行攻击，实现实体摧毁。通常情况下，在军用和非军用网

络空间领域内,首先对情报信息中心分发的信息进行研究判断,然后根据判断结果定下作战决心、拟制作战计划、部署作战部队、指挥作战行动、协调作战力量和评估作战效果,直至完成作战任务。

网络防御中心由网络空间监测预警系统、网络空间应急响应系统、网络空间恢复反击系统、网络空间防护系统组成;接收来自情报信息中心的网络空间动态信息,并进行态势评估,然后针对评估结果对相应的软件环境和实体环境进行调整和完善,并与网络攻击中心相互配合,寓攻于守,共同完成作战任务。支援保障中心不断地更新软件防护技术和安全防护措施。同时,网络防御中心与外部协调中心相互支援、配合,构筑网络空间防护屏障。网络防御中心负责对己方网络空间的威胁识别、危机告警和评估、网络伪装、密码防御、访问控制、防火墙构筑、网侵清除、网络隔离、安全备份、数据恢复、系统重构、入侵追踪、网络反击、安全防护、漏洞查补和隐患排查等,其利用监测预警系统监测己方网络空间的运行情况,防止敌方进行网络攻击、病毒入侵和电磁干扰。当出现异常情况,及时通过应急响应系统、恢复反击系统和防护系统的预置方案进行紧急处理,做到“发现”即“摧毁”,保持网络空间的软件和硬件环境时刻处于安全状态。

支援保障中心负责管理分配网络空间侦察、进攻和防御作战中所需要的频谱资源,研发革新攻防技术,更新换代作战装备和配备各类武器等保障活动。其对整个网络空间作战指挥提供技术和硬件支持,以确保网络空间指挥体系中各个要素频谱资源的合理分配,软件程序的更新、升级、换代,武器装备技术、战术优势的保持和其他作战指挥需求的满足。

外部协调中心下设网络舆情监察反馈系统、军地网络联合指挥系统和地方网络力量协调系统。其与情报信息中心形成了信息优势互补,共同构建信息数据库,辅助作战指挥的开展。同时,接受综合保障中心的技术与武器装备的支援,协同建立军方、地方进行技术与武器装备交流的纽带。外部协调中心主要负责协调控制非军事领域中的网络空间行动,利用互联网对敌方进行心理战和舆论战,破坏敌方军心、瓦解敌方斗志;对内做好舆论引导,防止敌方对己方舆论环境进行侵蚀、干扰和蛊惑、煽动。外部协调中心通过对地方网络力量的科学指挥与运用,使之有组织、有秩序和高效地参与网络空间作战行动,进而形成合力,共同打击敌方网络空间作战力量。

### 9.3.5 网络空间作战的组织结构设想方案

网络空间是一个极其错综庞杂的系统。其作战组织必须周密、详细、高效、顺畅,至少应满足传统组织的几项基本条件:①从组织的任何一个位置可以通向其他任何一个位置;②任何一个位置不能同时受两个不同的位置领导;③任何一个行动不能同时接受两个不同的指令指挥;④指令或反馈通路必须畅通无阻并且能保证时效。

网络空间作战的组织结构是网络空间作战指挥机构内部的部门设置。结构决定功能,指挥机构的编组对指挥机构指挥功能的形成和发挥有着重要影响。因此,进行网络空间作

战指挥机构的编组应遵循指挥机构编组相匹配的规律。只有优化组织结构，才能有利于联合战役网络空间作战指挥集中统一、简明高效。

网络空间作战指挥机构编组示意图如图 9-11 所示。整个机构编组由综合计划组、电子对抗组、实体摧毁控制组、网络作战组、信息安全保障组、心理战组、综合保障组。在网络作战组中主要设立指挥控制小组、计划协调小组、网络侦察小组、网络攻击小组、网络防御小组、网络监控小组、网络支援小组、决策咨询小组等。将综合计划和综合保障由网络空间作战机构统一协调，有利于从更高层次对网络空间作战力量的集中掌控和使用。

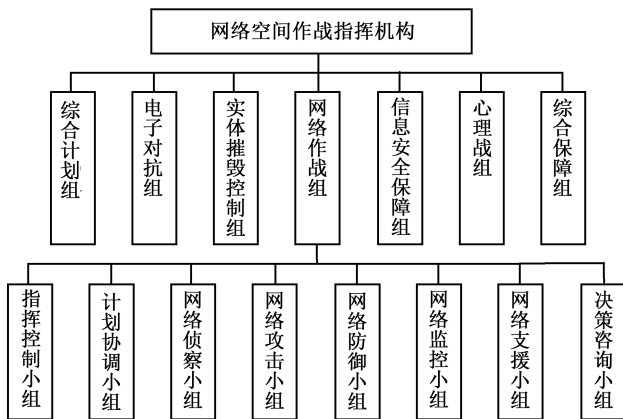


图 9-11 网络空间作战指挥机构编组示意图

综合计划组的职责为：①做好网络空间作战规划程序文件的编制、审核、管理和维护工作。②建立、健全、贯彻、实施、考核计划管理等各项制度及培训；③负责制定月、季、年度报表，以及作战计划和作战效益指标计划的编制，并协助检查、督办、考核；④统计、汇总、分析、动态完善及上报网络空间作战的信息；⑤协调、解决计划执行中出现的问题，并分析、预警、上报计划执行情况；⑥更新、维护计划管理系统相关数据信息。

电子对抗组负责电子战（包括电子情报、战区威慑、电子秩序）、通信侦察与反侦察、通信干扰与反干扰和电子防御等技术方面的工作。

实体摧毁控制组负责对敌方网络空间作战系统中要害目标的实体进行破坏、摧毁，以瘫痪敌作战系统。如摧毁敌人的指挥信息系统，或者摧毁敌人的通信枢纽和雷达站等指挥系统中的要害目标、节点目标、关键环节、“大脑”、“中枢”和“神经”系统。

信息安全保障组负责信息安全方针框架、规范、目标、流程、制度的制定；负责信息安全决策、管理、执行和监管；综合利用各种成熟的信息安全技术与产品，实现不同层次的身份鉴别、访问控制、数据完整性、数据保密性和抗抵赖等安全功能。通过安全运行管理，规范运行管理、安全监控、事件处理、变更管理过程，及时、准确、快速地处理安全问题，保障业务平台系统和应用系统的稳定可靠运行。通过周密的生产调度、安全运维管理、安全监测预警，及时排除安全隐患，确保业务系统持续、可靠地运行。针对各种突发灾难事件，对重要信息系统建立灾备系统，定期进行应急演练，形成快速响应、快速恢复的机制。最终达到保障信息安全、系统安全、物理安全和运行安全的目的。



心理战组的职责是利用人在对抗环境中的心理变化规律,借助传单、书报、广播、电影、电视、通信等媒介,采用声音、光线、形象、传媒、威慑、谋略、佯动、伪装、欺诈、恐吓、诱惑、诡诈、收买、谣言、宣传等手段,通过大量的信息传递,瓦解敌方士气,削弱抵抗意志,使其放弃抵抗、逃避战斗乃至缴械投降;最大限度地争取盟友,孤立对方,置对方于心理弱势和劣势;在本民族,本国家内部赢得民心民意,形成同仇敌忾的强大气势;以正义之师的形象激励参战人员斗志和士气,造成官兵的战场心理优势。

综合保障组职责是制定网络空间作战装备技术保障计划;协调与调拨指挥信息系统和网络空间作战设备,协调各种网络空间作战设备的维修与保障。

指挥控制小组主要职责是对上协助联合作战指挥员完成网络空间作战的决策、指挥、协调等任务,对下根据联合战役指挥员的指示和授权,负责具体的网络空间作战的组织指挥工作。

计划协调小组主要职责是筹划网络空间作战行动,拟制统一的网络空间作战计划;负责各种文电、计划的上传与下达;按指挥员的要求和网络空间作战计划,协调、控制网络空间作战群的作战行动;根据需要协调网络空间作战与其他常规作战行动以及网络攻击与防御行动。

网络侦察小组主要职责是搜集和处理与战役网络空间作战相关的情报,提出侦察报告建议,制订网络侦察计划,提出网络侦察建议,组织和协调战役网络侦察行动。

网络攻击小组主要职责是根据联合职责的需要,制订网络攻击行动计划;指挥协调各作战集团(群)网络攻击行动。

网络防御小组主要负责网络安全监测、防护行动的组织协调,军地计算机、电信、关键基础设施网络的安全防护。

网络监控小组主要负责网络空间舆论引导、政策宣传。利用互联网络及时了解和掌握网上国际舆论和国内舆论对己方战役的态度和支持率。及时监控敌方利用互联网对己方的不利宣传,配合政治、外交领域的斗争,组织网络空间舆论战、心理战等。

网络支援小组负责网络空间作战的决策支持、信息通报、网络通信保障和作战的效能评估。

决策咨询小组主要职责是协调解决军地信息网络安全问题和地方网络空间作战力量运用问题。

### 9.3.6 网络空间作战力量的编成考虑

网络空间作战力量的编成主要根据所担负任务来确定,如图9-12所示。

网络空间作战态势感知力量是网络空间战场的“观察者”,主要负责收集和处理网络空间中敌我双方相关活动的信息,并从物理设施层、信号电磁层、信息数据层和心理认知层4个层面对战场态势进行分析处理,为决策者提供信息支撑。

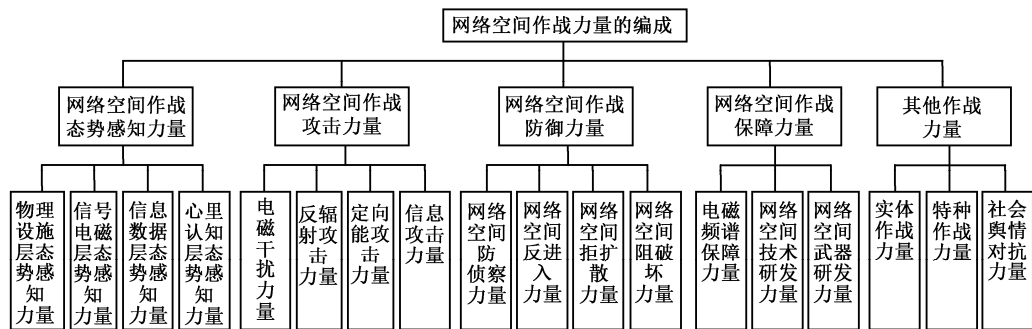


图 9-12 网络空间作战力量的编成

网络空间作战攻击力量主要开展对敌方网络空间进行破网、渗透和控制等一系列作战行动，同时配合防御系统对敌方网络攻击力量进行追踪，破坏敌方进攻行动，主要包括电磁干扰力量、反辐射攻击力量、定向能攻击力量和信息攻击力量。网络空间作战攻击力量是网络空间作战的“利剑”，其首要任务是破坏敌方网络、瘫痪敌方信息系统。

网络空间作战防御力量主要担负自身网络空间的安全防护，时刻警惕病毒入侵，保证自身网络的正常运行，主要包括网空间防侦察力量、反进入力量、拒扩散力量和阻破坏力量，在网络空间防御的各个阶段有针对性地采取措施，保证网络安全。

网络空间作战保障力量针对网络空间作战中各作战力量对频谱这一有限资源的利用需求统一规划部署、按需分配，协调做好频谱管理事宜，并结合技术或装备的支援需求，成立专门的网空间技术武器研发力量，并对网络空间作战力量进行考核，对网络空间作战进行评估，从软、硬件两方面对作战力量进行全面升级革新，适应战争发展趋势。

其他作战力量主要包括实体作战力量、特种作战力量和社会舆情对抗力量等。其中：实体作战力量主要针对敌方信息枢纽进行硬摧毁，与网络空间的软杀伤形成互补；特种作战力量主要针对敌方重要目标实施秘密潜入、内部信息获取等高难度任务；社会舆情对抗力量由地方掌握网络攻防技术的机构和人员组成，是网络空间作战力量的后备军。

## 附 录 英文缩略语及其中英文对照

缩略语	英 文 全 称	中 文
ACL	Access Control List	访问控制列表
ADCON	Administrative Control	行政控制
AESA	Active Electronically Scanned Array	有源电子扫描阵列
AH	Authentication Header	认证头标
API	Application Programming Interface	应用程序编程接口
ARP	Address Resolution Protocol	地址解析协议
APT	Advanced Persistent Threat	高级持续性威胁
B/S	Browser/Server	浏览器/服务器
BC	Boundary Controller	边界控制器
BGP	Border Gateway Protocol	边界网关协议
BIOS	Basic Input Output System	基本输入输出系统
C <sup>4</sup> ISR	Command、Control、Communication、Computer、Intelligence、 Surveillance、Reconnaissance	指挥、控制、通信、计算机、情报、 监视与侦察
C/S	Client/Server	客户端/服务器
CERT	Computer Emergency Response Team	计算机应急响应小组
CGI	Common Gateway Interface	公共网关接口
CIS	Caller Identification Server	身份识别服务器
CISIE	Caller Identification System in the Internet Environment	因特网环境身份识别系统
CITRA	Cooperative Intrusion Traceback and Response Architecture	协同入侵追踪和响应框架
CNCI	Comprehensive National Cybersecurity Initiative	国家网络安全综合计划
COCOM	Combatant Command	作战指挥
CPU	Central Processing Unit	中央处理器
CSA	Cyberspace Situation Awareness	网络空间态势感知
CSS	Cascading Style Sheets	层叠样式表
DAC	Discretionary Access Control	自主访问控制
DARPA	Defense Advanced Research Projects Agency	国防高级研究计划局
DC	Discovery Coordinator	发现协调器
DCO	Defensive Cyber Operations	防御性网络作战
DCT	Discrete Cosine Transform	离散余弦变换
DDoS	Distributed Denial of Service	分布式拒绝服务
DDR	Double Data Rate	双倍速率
DecIDUoS	Decentralized Source Identification for Network-Based Intrusions	网络入侵源点的安全管理识别
DES	Data Encryption Standard	数据加密标准
DFT	Discrete Fourier Transform	离散傅里叶变换

缩略语	英文全称	中文
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DHT	Discrete Hadmard transform	离散哈达玛特变换
DIDS	Distributed IDS	分布式入侵检测系统
DISA	Defense Information Systems Agenc	国防信息系统局
DLL	Design Limit Load	设计极限载荷
DMZ	Demilitarized Zone	隔离区
DNS	Domain Name System	域名系统
DoS	Denial of Service	拒绝服务
DOS	Disk Operating System	磁盘操作系统
DPI	Deep Packet Inspection	深度包检测
DPM	Deterministic Packet Marking	确定性包标记
DWT	Discrete Wavelet Transform	离散小波变换
EBP	Extend Base Pointer	扩展基址指针
ESP	Extend Stack Pointer	扩展堆栈指针
ETCPW	Extensional TCP Wrapper	扩展的 TCP 封装
EU	Europe	欧洲
FCC	Functional Combatant Commander	职能作战司令官
FE	Far East	远东地区
FTP	File Transfer Protocol	文件传送协议
GCC	Geographic Combatant Commander	地理作战司令官
GIG	Global Information Grid	全球信息栅格
GNOSC	Global NetOps and Security Center	全球网络作战与安全中心
HPM	High Power Microwave	高功率微波
HTML	HyperText Markup Language	超文本标记语言
HTTP	Hypertext Transport Protocol	超文本传送协议
IaaS	Infrastructure as a Service	基础设施即服务
ICMP	Internet Control Messages Protocol	因特网控制报文协议
ID	IDentifier	标识符
IDCT	Inverse DCT	逆离散余弦变换
IDIP	Intruder Detection and Isolation Protocol	入侵检测和隔离协议
IDS	Intrusion Detection System	入侵检测系统
IE	Internet Explorer	网页浏览器
IIS	Internet Information Server	因特网信息服务器
IP	Internet Protocol	网际协议
IPS	Intrusion Prevention System	入侵防御系统
IPSec	IP Security protocol	IP 安全协议
IPv4	IP version 4	第 4 版 IP
IPv6	IP version 6	第 6 版 IP
ISAKMP	Internet Security Association and Key Management Protocol	因特网安全关联和密钥管理协议
ISN	Initial Sequence Number	初始序列号
ISO	International Organization for Standardization	国际标准组织

缩略语	英文全称	中文
ISP	Internet Service Provider	因特网服务提供商
ISR	Intelligence、Surveillance、Reconnaissance	情报、监视和侦察
IT	Information Technology	信息技术
JDL	Joint Directorate of Laboratories	实验室理事联合会
JS	JavaScript	Java 描述语言
JVM	Java Virtual Machine	Java 虚拟机
LSB	The Least Significant Bits	最不重要比特位
MAC	Medium Access Control	介质访问控制
MAC	Mandatory Access Control	强制访问控制
MAC	Message Authentication Code	消息认证码
MBR	Main Boot Record	主引导记录
MD5	Message Digest Algorithm 5	信息摘要算法 5
ME	Middle East	中东
NAT	Network Address Translation	网络地址转换
NCPS	National Cybersecurity Protection System	国家网络安全保护系统
NCR	National Cyber Range	国家网络靶场
NGEN	Next Generation Enterprise Network	下一代企业网络
NGJ	Next Generation Jammer	下一代干扰机
NIOC	Navy Information Operations Command	海军信息战司令部
NOC	Network Operations Center	网络作战中心
NOSC	Network Operations and Security Center	网络作战与安全中心
NTFS	New Technology File System	新技术文件系统
OBAC	Object-Based Access Control	基于对象的访问控制
ONENET	Navy's Outside the Continental United States Enterprise Network	美国海军大陆企业网络
OPCON	Operational Control	作战控制
OSI	Open System Interconnect Reference Model	开放系统互联参考模型
PC	Personal Computer	个人计算机
PE	Portable Executable	可移植的执行体
PGP	Pretty Good Privacy	良好隐私
PKI	Public Key Infrastructure	公钥基础设施
PPM	Probabilistic Packet Marking	概率性包标记
QoS	Quality of Service	服务质量
RADIUS	Remote Authentication Dial In User Service	远程用户服务拨号认证
RAID	Redundant Arrays of Independent Disk	独立磁盘冗余阵列
RAT	Ram Air Turbine	冲压式空气涡轮
RBAC	Role-Based Access Control	基于角色的访问控制
RET	RETurn address	返回地址
RIP	Route Information Protocol	选路信息协议
RPC	Remote Procedure Call Protocol	远程过程调用协议
RPF	Reverse Path Forwarding	反向路径转发
RSA	Rivest-Shamir-Adelman	非对称加密算法
SA	Situation Awareness	态势感知

缩略语	英文全称	中文
SA	Security Associations	安全连接关系
SAN	Storage Area Network	存储区域网络
SCADA	Supervisory Control And Data Acquisition	监控与数据采集
SCSI	Small Computer System Interface	小型计算机系统接口
SD	Super Disc	超级光盘
SDN	Software Defined Network	软件定义网络
SMTP	Simple Mail Transfer Protocol	简单邮件传输协议
SNMP	Simple Network Management Protocol	简单网络管理协议
SQL	Structured Query Language	结构化查询语言
SSL	Secure Socket Layer	安全套接层
SSN	Security Server Network	安全服务器网络
SWT	Sleepy Watermark Tracing	休眠水印追踪
TACON	Tactical Control	战术控制
TBAC	Task-Based Access Control	基于任务的访问控制
TCP	Transport Control Protocol	传输控制协议
TNCC	Theater Network Operations Control Center	战区网络作战控制中心
TNOSC	Theater NetOps and Security Center	战区网络作战与安全中心
TTP	Tactics, Techniques and Procedures	战术、技术和规程
TTL	Time To Live	生存时间
UDP	User Datagram Protocol	用户数据报协议
UHF	Ultra High Frequency	超高频
UML	Unified Modeling Language	统一建模语言
URL	User Route List	用户路由表
VHF	Very High Frequency	甚高频
VLAN	Virtual Local Area Network	虚拟局域网
VM	Virtual Machine	虚拟机
VPN	Virtual Private Network	虚拟专用网
WWW	World Wide Web	万维网
XSS	Cross Site Scripting	跨站脚本

## 参考文献

- [1] 惠志斌, 覃庆玲. 网络空间安全蓝皮书: 中国网络空间安全发展报告 (2016) [R]. 北京: 社会科学文献出版社, 2016.
- [2] 蒋天发, 苏永红. 网络空间信息安全[M]. 北京: 电子工业出版社, 2017.
- [3] 杨林, 于全. 动态赋能网络空间防御[M]. 北京: 人民邮电出版社, 2016.
- [4] 刘峰, 林东岱等. 美国网络空间安全体系[M]. 北京: 科学出版社, 2015.
- [5] [美]保罗·沙克瑞恩 (Paulo Shakarian), 亚娜·沙克瑞恩 (Jana Shakarian), 安德鲁·鲁夫 (Andrew Ruef). 网络战: 信息空间攻防历史、案例与未来[M]. 吴奕俊等, 译. 北京: 金城出版社, 2016.
- [6] 张笑容. 第五空间战略: 大国间的网络博弈[M]. 北京: 机械工业出版社, 2014.
- [7] 张显龙. 中国网络空间战略[M]. 北京: 电子工业出版社, 2015.
- [8] 吕晶华. 美国网络空间战思想研究[M]. 北京: 军事科学出版社, 2014.
- [9] 方兴东, 胡怀亮. 网络强国——中美网络空间大博弈[M]. 北京: 电子工业出版社, 2014.
- [10] [美]Sushil Jajodia, Peng Liu, Vipin Swarup, Cliff Wang. 网络空间态势感知问题与研究[M]. 余健, 游凌, 樊龙飞, 周德川, 译. 北京: 国防工业出版社, 2014.
- [11] 吴礼发, 洪征, 李华波. 网络攻防原理与技术 (第2版) [M]. 北京: 机械工业出版社, 2017.
- [12] 何精华. 网络空间的政府治理[M]. 上海: 上海社会科学院出版社, 2006.
- [13] 祝世雄, 陈周国, 张小松, 陈瑞东. 网络攻击追踪溯源[M]. 北京: 国防工业出版社, 2015.
- [14] 天河文化. 黑客攻防从入门到精通 (攻防与脚本编程篇) [M]. 北京: 机械工业出版社, 2015.
- [15] 明月工作室, 赵玉萍. 黑客攻防从入门到精通 (应用大全篇·全新升级版) [M]. 北京: 北京大学出版社, 2017.
- [16] [美]Charlie Miller, Dionysus Blazakis, Dine Dai Zovi, Stefan Esser, Vincenzo Iozzo, Ralf-Philipp We. 黑客攻防技术宝典: iOS 实战篇[M]. 傅尔也, 译. 北京: 人民邮电出版社, 2013.
- [17] 武新华, 孙振辉. 最新黑客攻防实战从入门到精通 (第二版) [M]. 北京: 科学出版社, 2011.
- [18] 陈小兵, 刘晨, 黄小波. 黑客攻防: 实战加密与解密[M]. 北京: 电子工业出版社, 2016.
- [19] [美]Ed Skoudis, Tom Liston. 黑客攻防演习 (第二版) [M]. 龚玲, 张云涛, 郝黎明, 李敏, 译. 北京: 电子工业出版社, 2007.
- [20] 王叶. 黑客攻防大全[M]. 北京: 机械工业出版社, 2015.
- [21] 马林立. 外军网电空间战——现状与发展[M]. 北京: 国防工业出版社, 2012.
- [22] 王国良, 鲁智勇等. 信息网络安全测试与评估[M]. 北京: 国防工业出版社, 2015.

- [23] 王晋东, 张恒巍, 王娜, 徐开勇. 信息系统安全风险评估与防御决策[M]. 北京: 国防工业出版社, 2017.
- [24] 姚淑萍等. 网络安全预警防御技术[M]. 北京: 国防工业出版社, 2015.
- [25] Greg Holden. 网络防御与安全对策[M]. 黄开枝、孙岩等, 译. 北京: 清华大学出版社, 2004.
- [26] 兰巨龙, 程东年, 刘文芬, 胡宇翔, 于洪涛, 李玉峰, 陈越. 信息网络安全与防护技术[M]. 北京: 人民邮电出版社, 2014.
- [27] 马丁·C. 理贝基(兰德公司). 网络威胁与网络战[M]. 李格非, 王君, 译. 北京: 军事宜文出版社, 2010.
- [28] 甘刚, 曹获花, 王敏, 王祖俪, 张永波. 网络攻击与防御[M]. 北京: 清华大学出版社, 2008.
- [29] [美]肖恩·S.柯斯蒂根(Sean S. Costigan), 杰克·佩里(Jake Perry). 赛博空间与全球事务[M]. 饶岚, 梁玥等, 译. 北京: 电子工业出版社, 2013.
- [30] 柯宏发, 唐跃平, 李云涛, 夏斌, 徐勇, 祝冀鲁. 赛博空间作战蓝军力量建设概论[M]. 北京: 国防工业出版社, 2016.
- [31] 孙义明, 李魏. 赛博空间——新的作战域[M]. 北京: 国防工业出版社, 2014.
- [32] [美]克里斯·麦克纳布(Chris McNab). 网络安全评估(第二版)[M]. 王景新, 译. 北京: 中国电力出版社, 2010.
- [33] 李贺华. 信息安全等级保护与风险评估[M]. 北京: 水利水电出版社, 2014.
- [34] 郭璇, 肖治庭. 现代网络战[M]. 北京: 国防大学出版社, 2016.
- [35] [美]Christopher Paul. 信息战理论与实践[M]. 董宝良, 蔡磊, 李忠群等, 译. 北京: 电子工业出版社, 2015.
- [36] 贺雪晨. 信息对抗与网络安全(第3版)[M]. 北京: 清华大学出版社, 2015.
- [37] 胡建伟, 汤建龙, 杨绍全. 网络对抗原理[M]. 西安: 西安电子科技大学出版社, 2004.
- [38] 李继斌. 联合战役网络空间作战指挥问题研究[M]. 北京: 国防大学出版社, 2016.